CardMate By WASH GEAR
Carwash Activation System™

PA-DSS Implementation Guide

This PA-DSS Implementation guide is disseminated to customers, resellers and integrators through a link to the current version within the CardWorks application as well as www.washgear.com

This PA-DSS Implementation guide is reviewed on an annual basis and when new payment application versions are released, and updated as needed.

During the annual review this document is also updated as needed to document changes to the underlying PA-DSS requirements.

Table of Contents

Revision Information

Name	Title	Date of Update	Summary of Changes

Note: This PA-DSS Implementation Guide is disseminated to customers, resellers and integrators through a link to the current version within the CardWorks application as well as www.washgear.com

This PA-DSS Implementation guide is reviewed on an annual basis and when new payment application versions are released, and updated as needed.

During the annual review this document is also updated as needed to document changes to the underlying PA-DSS requirements.

Guide is reviewed on a yearly basis. Updates should be tracked and reasonable accommodations should be made to distribute or make the updated guide available to users.

Executive Summary

CardWorks version 3.0has been PA-DSS (Payment Application Data Security Standard) certified. For the PA-DSS assessment, we worked with the following PCI SSC approved Payment Application Qualified Security Assessor (PAQSA):

Assessor

Coalfire Systems, Inc.

150 Nickerson Street Suite 106

Seattle, WA 98109

This document also explains the Payment Card Industry (PCI) initiative and the Payment Application Data Security Standard (PA-DSS) guidelines. The document then provides specific installation, configuration, and ongoing

management best practices for using Payment Application as a PA-DSS validated Application operating in a PCI Compliant environment.

PCI Security Standards Council Reference Documents

The following documents provide additional detail surrounding the PCI SSC and related security programs (PA-DSS, PCI DSS, etc):

Payment Applications Data Security Standard
https://www.pcisecuritystandards.org/tech/pa-dss.htm

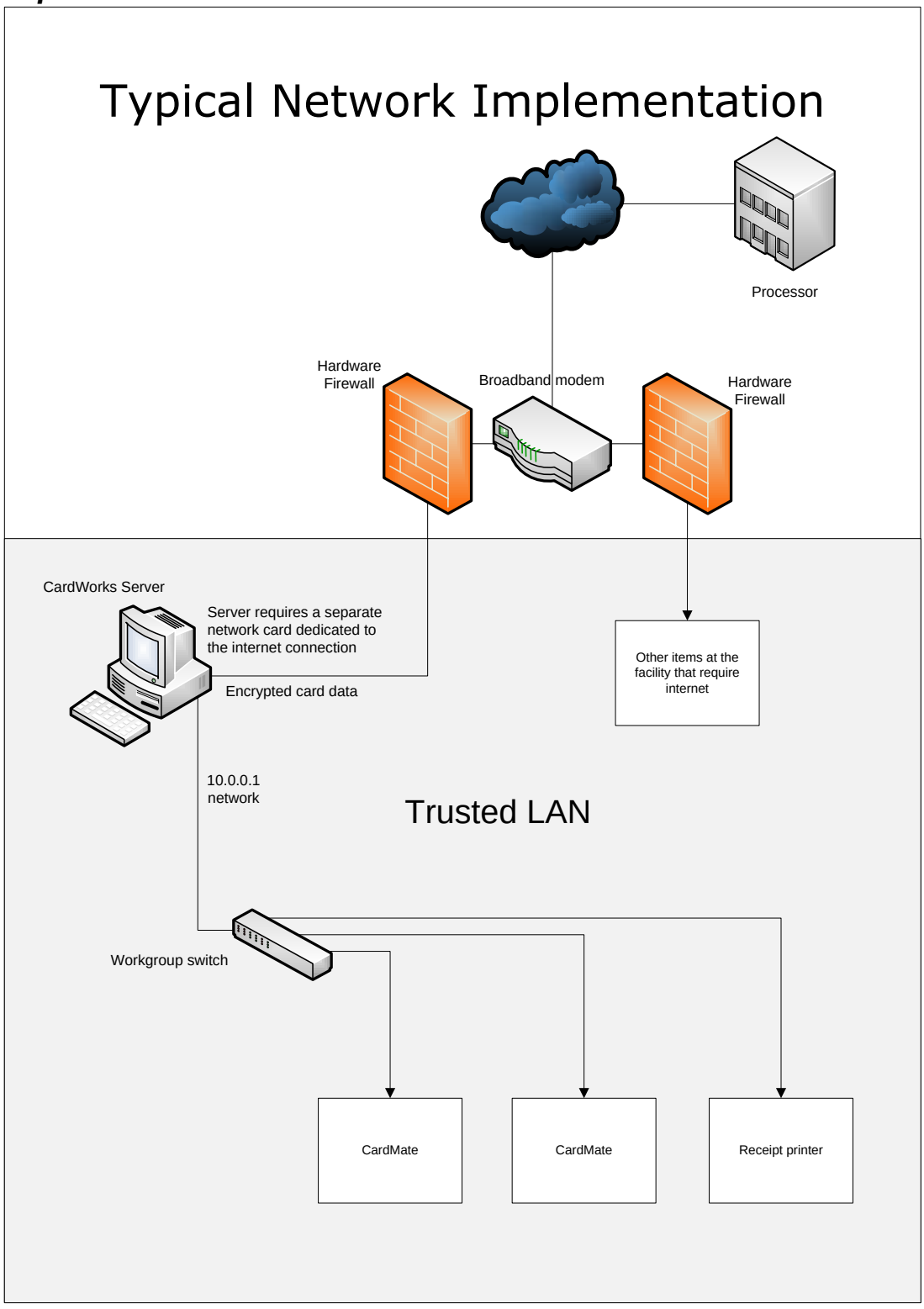
PCI DSS
https://www.pcisecuritystandards.org/tech/download_the_pci_dss.htm

Open Web Application Security Project (OWASP)
http://www.owasp.org

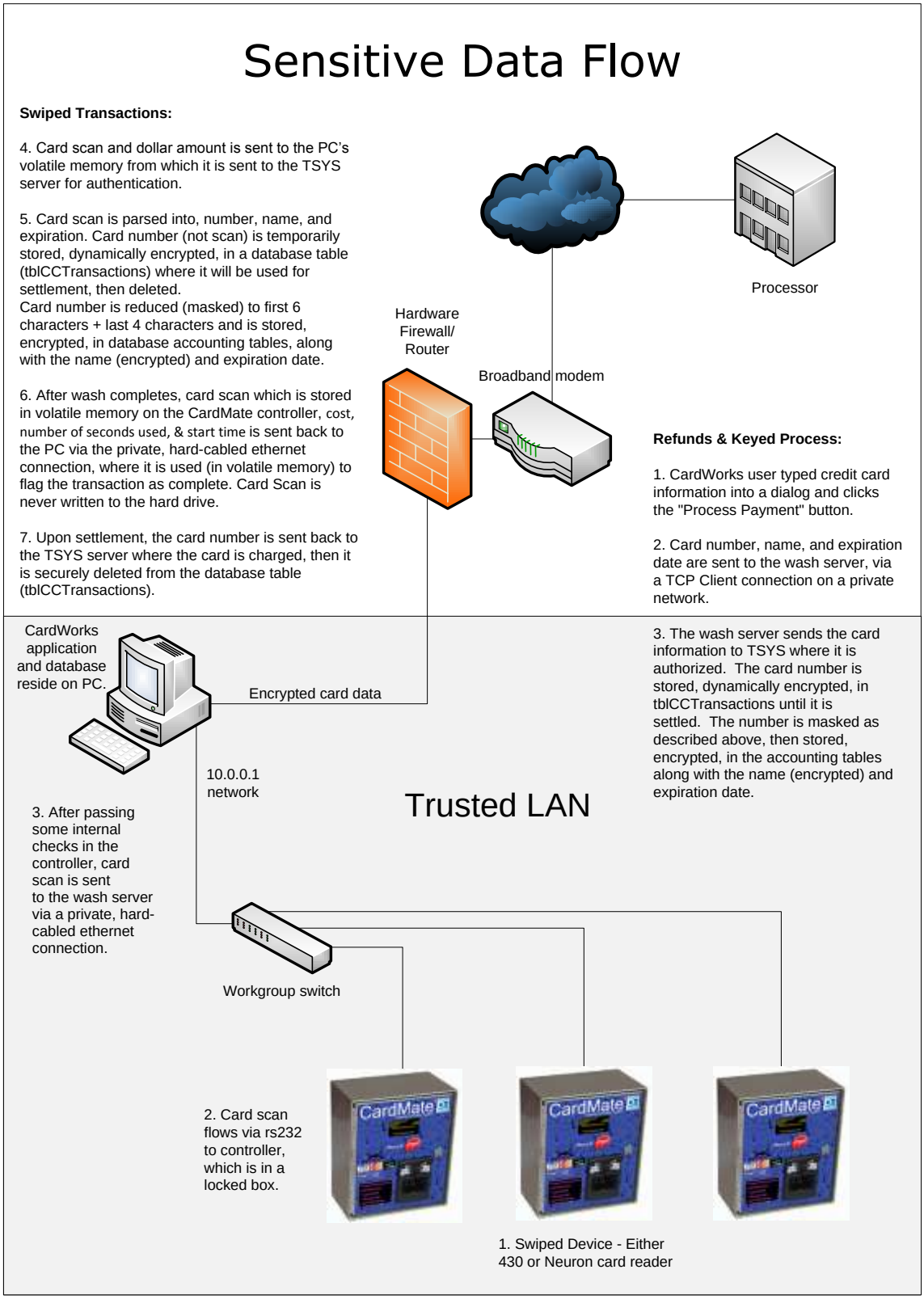
Application Summary

Name:	CardWorks & CardMate
Specific File Version Numbers:	3.0
Credit cards server:	TSYS
Interface:	Vital/TSYS Integrator V4 .NET Edition
Operating Systems:	Windows Vista, XP
Code base DB engine:	Microsoft SQL Server Express
Application Description:	CardWorks software and CardMate hardware serve to facilitate the acceptance of credit cards and proprietary fleet and gift cards as an alternative to coins as a means to activate equipment within a self serve car wash and. CardWorks also serves as an accounting and reporting tool for the car wash owner.
Application Environment	The CardWorks payment application works in concert with the CardMate hardware in a secure local network which is isolated from the internet network via a separate network card dedicated to handing local traffic between the CardMate hardware and the PC.

Typical Network Implementation



Dataflow Diagram



Difference between PCI Compliance and PA-DSS Validation

As a software vendor, our responsibility is to be “PA-DSS Validated.”

We have performed an assessment and certification compliance review with our independent assessment firm, to ensure that our platform does conform to industry best practices when handling, managing and storing payment related information.

PA-DSS is the standard against which Payment Application has been tested, assessed, and validated.

PCI Compliance is then later obtained by the merchant, and is an assessment of your actual server (or hosting) environment.

Obtaining “PCI Compliance” is the responsibility of the merchant and your hosting provider, working together, using PCI compliant server architecture with proper hardware & software configurations and access control procedures.

The PA-DSS Validation is intended to ensure that the Payment Application will help you achieve and maintain PCI Compliance with respect to how Payment Application handles user accounts, passwords, encryption, and other payment data related information.

The Payment Card Industry (PCI) has developed security standards for handling cardholder information in a published standard called the PCI Data Security Standard (DSS). The security requirements defined in the DSS apply to all members, merchants, and service providers that store, process or transmit cardholder data.

The PCI DSS requirements apply to all system components within the payment application environment which is defined as any network device, host, or application included in, or connected to, a network segment where cardholder data is stored, processed or transmitted.

The 12 Requirements of the PCI DSS:

Build and Maintain a Secure Network

1. Install and maintain a firewall configuration to protect data
2. Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

3. Protect Stored Data
4. Encrypt transmission of cardholder data and sensitive information across public networks

Maintain a Vulnerability Management Program

5. Use and regularly update anti-virus software
6. Develop and maintain secure systems and applications

Implement Strong Access Control Measures

7. Restrict access to data by business need-to-know
8. Assign a unique ID to each person with computer access
9. Restrict physical cardholder data

Regularly Monitor and Test Networks

10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes

Maintain an Information Security Policy

12. Maintain a policy that addresses information security

Responsible Parties—PA-DSS

Customers

Customers are merchants, service providers, or others who buy or receive a third-party payment application to store, process, or transmit cardholder data as part of authorizing or settling of payment transactions. Customers are responsible for:

- Implementing a PA-DSS-compliant payment application into a PCI DSS-compliant environment;
- Configuring the payment application (where configuration options are provided) according to this *PA-DSS Implementation Guide* provided by the vendor;
- Configuring the payment application in a PCI DSS-compliant manner;
- Maintaining the PCI DSS-compliant status for both the environment and the payment application configuration.

Resellers and Integrators

Resellers and integrators are those entities that sell, install, and/or service payment applications on behalf of software vendors or others. Resellers and integrators are responsible for:

- Implementing a PA-DSS-compliant payment application into a PCI DSS-compliant environment (or instructing the merchant to do so)
- Configuring the payment application (where configuration options are provided) according to this *PA-DSS Implementation Guide* provided by the vendor; (No configuration required within CardWorks)
- Configuring the payment application (or instructing the merchant to do so) in a PCI DSS-compliant manner; (No configuration required within CardWorks)
- Servicing the payment applications (for example, troubleshooting, delivering remote updates, and providing remote support) according to the *PADSS Implementation Guide* and PCI DSS.

Vendors

Vendors are those who develop payment applications that store, process, or transmit cardholder data as part of authorization or settlement, and then sell, distribute, or license these payment applications to third parties (customers or resellers/integrators). Vendors are responsible for:

- Creating PA-DSS compliant payment applications that facilitate and do not prevent their customers' PCI DSS compliance. (The application cannot require an implementation or configuration setting that violates a PCI DSS requirement.).
- Following PCI DSS requirements whenever the vendor stores, processes or transmits cardholder data (for example, during customer troubleshooting);
- Creating a *PA-DSS Implementation Guide*, specific to each payment application.
- Educating customers, resellers, and integrators on how to install and configure the payment applications in a PCI DSS-compliant manner; (This PA-DSS Implementation guide)
- Ensuring payment applications meet PA-DSS by successfully passing a PA-DSS review as specified in this document.

Certain operating system and router settings may prohibit PCI DSS compliance.

These settings cannot be controlled by the payment application vendor and are the responsibility of the customer, not the payment application vendor.

Considerations for the Implementation of Payment Application in a PCI-Compliant Environment

The following areas must be considered for proper implementation in a PCI-Compliant environment.

Sensitive Credit Card Data requires special handling

Remove Historical Credit Card Data

Set up Good Access Controls

Properly Train and Monitor Admin Personnel

Key Management Roles & Responsibilities

PCI-Compliant Remote Access

Use SSH, VPN, or SSL/TLS for encryption of administrative access

Log settings must be compliant

PCI-Compliant Wireless settings

Data Transport Encryption

PCI-Compliant Use of Email

Network Segmentation

Never store cardholder data on internet-accessible systems

Use SSL for Secure Data Transmission

Delivery of Updates in a PCI Compliant Fashion

PA-DSS 1.1.4 Delete sensitive authentication data stored by previous payment application versions

- Historical data must be removed (magnetic stripe data, card validation codes, PINs, or PIN blocks stored by previous versions of the payment application)
- **Such removal is absolutely necessary for PCI DSS compliance**

- **How to remove historical data**
  - CardWorks includes capabilities to securely wipe sensitive cardholder data.
  - CardWorks version 3.0 and later securely deletes CardWorks data files created by CardWorks versions prior to 3.0 automatically provided they still reside in their original installed location. Previous versions of CardWorks allowed for the historical retention of swipe data, validation values or codes.

  - If you are unsure where backup files created in versions prior to 3.0 reside, WashGear recommends using the search tool within Windows to find all files named transactions, visaauth, visacapt, visanet, visadial, visatcp and visaparm. Once the location of these files has been determined use the secure deletion tool within CardWorks to remove them as described below.

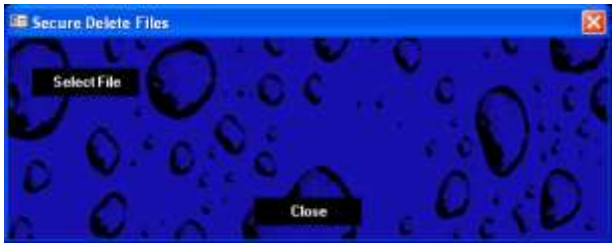
  - To assure all sensitive data from versions prior to CardWorks 3.0 are removed, delete all files listed using the secure deletion utility or the standalone version from your CardWorks installation CD Named “Secure Delete Tool.exe”

Secure File Deletion utility

You must be logged in as an administrator to access the secure deletion utility in CardWorks.

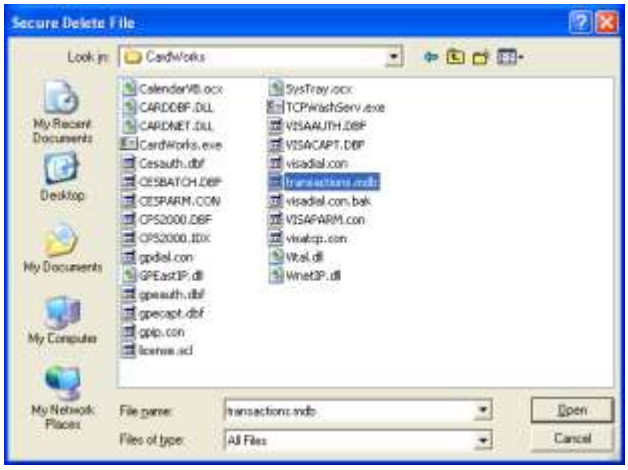
Click Tools> Secure Delete Files

Click Select File



Click the file you would like to delete then click open.

The file will be permanently and securely deleted.



By default, CardWorks versions prior to 3.0 store data in the following directories. These files need to be deleted manually if the computer is retired when implementing CardWorks version 3.0 otherwise these files will automatically be securely deleted by CardWorks 3.0 or higher upon installation.

WindowsVista;

C:\Users\"User Folder"\AppData\Local\VirtualStore\Program Files\WashGear\CardWorks

&

C:\Program Files\WashGear\CardWorks

WindowsXP:

C:\Program Files\WashGear\CardWorks

Backups:

Use this utility to delete any backup of CardWorks data files stored in locations other than those listed above.

PA-DSS 1.1.5 Delete any sensitive authentication data (pre-authorization) gathered as a result of troubleshooting the payment application.

- Sensitive authentication data (preauthorization) must only be collected when needed to solve a specific problem
    - When required, this data should only by collected by WashGear at the system Admin's request over a secure connection to WashGear tech support
- Such data must be stored only in specific, known locations with limited access.
    - WashGear will fulfill this requirement by storing the data in a confidential folder on the support person's work station, specified by WashGear solely for this purpose. The work

station is password protected to enforce access control, and the sensitive data is securely deleted immediately after use.

- Only collect a limited amount of such data as needed to solve a specific problem
- Sensitive authentication data must be encrypted while stored
    - WashGear will fulfill this requirement.
- **Such data must be securely deleted immediately after use**
    - WashGear will fulfill this requirement.

PA-DSS 2.1 Purge cardholder data after customer-defined retention period.

- Cardholder data must be purged after it exceeds the customer-defined retention period
    - CardWorks only retains sensitive data until daily settlement and the data is encrypted while stored between the time of authorization and settlement. As per requirement 2.1 of the PA-DSS the customer defined retention period of 24 hours is defined by the design of CardWorks.
- All locations where payment application stores cardholder data
    - CardWorks stores card holder data in the databases in the CardWorks folder which resides at C:\WashGear
        - This data is encrypted by CardWorks before being stored
        - In the case of a PC replacement you must securely delete this directory from the original hard drive using the secure deletion tool within CardWorks once the latest backup old PC has been restored on the new PC.

PA-DSS 2.7 Delete cryptographic key material or cryptograms stored by previous payment application versions.

- Cryptographic material must be removed
    - No previous version of CardWorks has ever stored any cryptographic materials or cryptograms which fulfills this requirement.
- How to remove cryptographic material
    - There are no cryptographic materials or cryptograms to remove
- Such removal is absolutely necessary for PCI compliance
    - There are no cryptographic materials or cryptograms to remove
- How to re-encrypt historic data with new keys
    - The key encryption key (KEK) can be changed and data re-encrypted by an Admin user at any time. To do so Click Tools> Re-Encrypt

PA-DSS 3.1 Use unique user IDs and secure authentication for administrative access and access to cardholder data.

- Do not use default administrative accounts for payment application logins.
    - Set unique usernames and passwords for both administrators and basic users within CardWorks before accepting credit cards.
- Assign secure authentication to default accounts (even if not used), and disable or do not use the accounts.
    - Set the default Admin account within CardWorks as inactive after adding the first legitimate Admin account.
- Use secure authentication for the payment application and system whenever possible.
    - Set up password protected administrative and basic user accounts in windows.
    - Set up administrative and basic user accounts in CardWorks.
- How to create secure authentication to access the payment application, per PCI DSS Requirements 8.5.8 through 8.5.15.
    - PCI-DSS 8.5.8 Do not use group, shared, or generic accounts and passwords to protect CardWorks.
    - PCI-DSS 8.5.9 Change user passwords at least every 90 days
    - PCI-DSS 8.5.10 Require a minimum password length of at least seven characters (CardWorks forces you to do this)
    - PCI-DSS 8.5.11 Use passwords containing both numeric and alphabetic characters (CardWorks forces you to do this)
    - PCI-DSS 8.5.12 Do 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
    - PCI-DSS 8.5.13 Limit repeated access attempts by locking out the user ID after not more than six attempts (CardWorks does this for you)
    - PCI-DSS 8.5.14 Set the lockout duration to thirty minutes or until administrator enables the user ID (CardWorks does this for you)
    - PCI-DSS 8.5.15 If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal. (CardWorks does this for you)
- Changing “out of the box” installation settings for unique user IDs and secure authentication will result in non-compliance with PCI DSS.
    - CardWorks has no settings that would disable the requirement for unique user IDs or secure authentications.

PA-DSS 3.2 Use unique user IDs and secure authentication for access to PCs, servers, and databases with payment applications.

Customers and resellers/integrators are strongly advised to control access, via unique user ID and PCI DSS-compliant secure authentication, to any PCs, servers, and databases with payment applications and cardholder data. In particular, customers and resellers/integrators are advised as follows:

- Implement unique usernames and passwords for both administrators and basic users within the CardWorks application before accepting credit cards.
- Do not use default administrative accounts for payment application logins or associated/required application software (for example, don't use the "sa" account for payment application access to SQL Server database).
- You must assign secure authentication to all default accounts (even if they won't be used), and then disable or do not use the accounts.
- You must assign secure authentication for payment applications and systems (including operating systems on which payment applications are running) whenever possible.
- Changing "out of the box" installation settings for unique user IDs and secure authentication will result in non-compliance with PCI DSS. (Note that it is not possible to disable secure authentication settings in the CardWorks application.)
- You must create PCI DSS-compliant secure authentication to access the payment application, per PCI DSS Requirements 8.5.8 through 8.5.15 as follows:
    - PCI-DSS 8.5.8 Do not use group, shared, or generic accounts and passwords to protect CardWorks
    - PCI-DSS 8.5.9 Change user passwords at least every 90 days (CardWorks enforces this.)
    - PCI-DSS 8.5.10 Require a minimum password length of at least seven characters (CardWorks enforces this.)
    - PCI-DSS 8.5.11 Use passwords containing both numeric and alphabetic characters (CardWorks enforces this.)
    - PCI-DSS 8.5.12 Do 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 (CardWorks enforces this.)
    - PCI-DSS 8.5.13 Limit repeated access attempts by locking out the user ID after not more than six attempts (CardWorks enforces this.)
    - PCI-DSS 8.5.14 Set the lockout duration to thirty minutes or until administrator enables the user ID (CardWorks enforces this.)
    - PCI-DSS 8.5.15 If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal. (CardWorks enforces this.)

PA-DSS 4.2 Implement automated audit trails.

- Set PCI DSS-compliant log settings, per PCI DSS Requirement 10
    - There is no way to turn this feature off within CardWorks so no action is needed on the part of the user.
    - Application logs are designed to fulfill PCI-DSS requirements 10.2.1-10.2.7 and 10.3.1-10.3.6
        - PCI-DSS 10.2.1 All individual accesses to cardholder data
        - 10.2.2 All actions taken by any individual with root or administrative privileges
        - 10.2.3 Access to all audit trails
        - 10.2.4 Invalid logical access attempts
        - 10.2 5 Use of identification and authentication mechanisms
        - 10.2.6 Initialization of the audit logs
        - 10.2.7 Creation and deletion of system-level objects
        - 10.3.1 User identification
        - 10.3.2 Type of event
        - 10.3.3 Date and time
        - 10.3.4 Success or failure indication
        - 10.3.5 Origination of event
        - 10.3.6 Identity or name of affected data, system component, or resource
- Application logging is required to maintain PCI compliance and disabling it in any way will result in non-compliance to PCI DSS.
- Disabling application logging should not be done and will result in non-compliance with PCI DSS.

PA-DSS 6.1 Securely implement wireless technology.

- If wireless is used within payment environment, install a firewall per PCI DSS Requirement 1.2.3.
    - PA-DSS1.2.3 Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.
    - PA-DSS 2.1.1 For wireless environments connected to the cardholder data environment or transmitting cardholder data, change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings. Ensure wireless device security settings are enabled for strong encryption technology for authentication and transmission.
    - *For new wireless implementations, it is prohibited to implement WEP after March 31, 2009.*
    - *For current wireless implementations, it is prohibited to use WEP after June 30, 2010.*
    - Wireless communication on the 10.0.0.1 network is **NOT supported by WashGear.**

- **Do not use wireless technology between the PC and any CardMate terminal.** CardWorks communicates to the card processor using SSL security as part of fulfilling this requirement but merchant must follow all the guidelines for securing a wireless connection to the PC running CardWorks to remain compliant.
-

PA-DSS 6.2 Secure transmissions of cardholder data over wireless networks.

- If payment application is implemented into a wireless environment, use PCI DSS-compliant wireless settings, per PCI DSS Requirement 4.1.1, 1.2.3 and 2.1.1
    - PCI-DSS 4.1.1 Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission.
        - *For new wireless implementations, it is prohibited to implement WEP after March 31, 2009.*
        - *For current wireless implementations, it is prohibited t0 use WEP after June 30, 2010.*
    - PA-DSS1.2.3 Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.
    - PA-DSS 2.1.1 For wireless environments connected to the cardholder data environment or transmitting cardholder data, change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings. Ensure wireless device security settings are enabled for strong encryption technology for authentication and transmission.
        - Wireless encryption keys must be changed anytime someone with knowledge of the keys leaves the company (PCI DSS 2.1.1)
        - Wireless encryption keys must be changed anytime someone with knowledge of the keys changes positions (PCI DSS 2.1.1)
        - Firmware on wireless devices must be updated to support strong encryption for authentication and transmission over wireless networks (e.g. WPA/WPA2) (PCI DSS 2.1.1)
    - Wireless communication on the 10.0.0.1 network is not supported by WashGear.
        - Do not use wireless technology between the PC and any CardMate terminals.
    - CardWorks communicates to the card processor using SSL security as part of fulfilling this requirement but merchant must follow all the guidelines for securing a wireless connection to the PC running CardWorks to remain compliant if internet service is being provided via wireless connection.

PA-DSS 9.1 Store cardholder data only on servers not connected to the Internet.

- Do not store cardholder data on Internet-accessible systems (for example, web server and database server must not be on same server).
    - Do not store cardholder data on Internet-accessible systems (e.g., web server and database server must not be on same server).
        - Never connect the internet to the ethernet switch on the 10.0.0.1 network.
        - Connect the internet & the 10.0.0.1 networks as specified in the network diagram contained in this guide.
        - Use separate network adapter cards in the PC to isolate the internet network from the 10.0.0.1 network & don't plug any internet cable into the 10.0.0.1 network switch.
    - WashGear does not provide any type of web servers, web components or web-based applications.
        - WashGear does not deliver any web components nor does it require web servers in the merchant network. Thus there is no need for a DMZ to be implemented in the merchant network. The typical merchant network is segmented from the public internet with an appropriately configured firewall. The database server runs on the same server as the WashGear application and the database is secured from outside access by disabling remote connections in SQL Express for all WashGear installations. If these settings are changed, you may become out of compliance with PCI DSS. If you (the merchant) require a web server for serving up content to the public internet, you must follow all guidance for establishing a properly secured DMZ to protect the cardholder data environment. Not doing so may bring you out of compliance with PCI DSS."
        - **If the merchant chooses to implement such software it must follow the network guidance provided elsewhere in this Implementation Guide and that cardholder data must never be stored on internet-accessible systems (i.e. web server and db server must never be on the same server).**

PA-DSS 10.1 Securely deliver remote payment application updates.

- WashGear does not typically connect to the merchant network remotely for the purposes of delivering software installs or updates. There are special circumstances which may require WashGear to do so. When this is required, the following guidelines must be followed to secure these remote connections.
- Receive remote payment application updates via secure modems, per PCI DSS Requirement 12.3.9

- PCI-DSS 12.3.9 Activation of remote-access technologies for vendors only when needed by vendors, with immediate deactivation after use.
    - WashGear uses Mikogo to connect to customers sites when necessary. There is no way to connect to another computer using Mikogo without permission being granted by the remote user at the time of connection.
    - By design Mikogo requires WashGear to obtain a unique meeting ID for each connection. This meeting ID must be entered by the user requesting support before any connection can be established. This user ID expires in 15 minutes if not used. In addition Mikogo requires the person requesting support to give permission to support staff to see the remote screen and a separate permission to control the mouse/keyboard.
    - Once support session is complete, the meeting must be ended by right clicking the Mikogo icon in the system tray, clicking "Quit meeting" selecting "End the meeting for all" and clicking OK. This can be done by either party in the connection.

- During application startup the application polls a secure web site to determine if an update is available. If so, the update is automatically downloaded from the same site and installed.
    - Installation and updates use a signed SSL certificate for both the installation and application manifests. The application will not install, update, or even run if the manifests that exist on the client do not authenticate against the manifests at the installation site.
    - Application users must be authenticated Windows users

- If computer is connected via VPN or other high speed connection, receive remote payment application updates via a firewall or a personal firewall per PCI DSS Requirement 1 or 1.3.9.
    - Establish firewall and router configuration standards that include the following:
        - PCI-DSS 1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations
            - This can be verified by a Qualified Security Assessors (QSAs)
        - PCI-DSS 1.1.2 Current network diagram with all connections to cardholder data, including any wireless networks
            - A standard network diagram is included in this PA-DSS Implementation guide. If your network is configured differently create a diagram that matches your network configuration.
        - PCI-DSS 1.1.3 Maintain a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone
            - Maintain a firewall between the PC and the internet, Most DSL & cable modems have integrated firewalls though you'll need to make sure any unnecessary or insecure services or protocols are not enabled, or are justified and documented as to appropriate use of the service. For example, FTP is not used, or is encrypted via SSH or other technology. CardWorks uses TCP/IP protocol and port 5003. Web browsers use HTTP protocol & port 80.

- PCI-DSS 1.1.4 Description of groups, roles, and responsibilities for logical management of network components
    - Document who has access to the PC, CardWorks and network components and what their responsibilities are.
- PCI-DSS 1.1.5 Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure
    - Document and justify the use of any service, protocol or ports being used that are not required by CardWorks or a web browser. CardWorks uses TCP/IP protocol and port 5003. Web browsers use HTTP protocol & port 80.
- PCI-DSS 1.1.6 Requirement to review firewall and router rule sets at least every six months
    - This can be verified by a Qualified Security Assessors (QSAs)
- PCI-DSS 1.2 Build a firewall configuration that restricts connections between untrusted networks and any system components in the cardholder data environment.
    - PCI-DSS 1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.
    - PCI-DSS 1.2.2 Secure and synchronize router configuration files.
        - Store a back up of the router configuration in the administrator's "My Documents" folder named as such.
    - PCI-DSS 1.2.3 Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.
        - Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment. CardWorks uses TCP/IP protocol and port 5003. Web browsers use HTTP protocol & port 80.
- PCI-DSS 1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.
    - PCI-DSS 1.3.1 Implement a DMZ to limit inbound and outbound traffic to only protocols that are necessary for the cardholder data environment.
    - PCI-DSS 1.3.2 Limit inbound Internet traffic to IP addresses within the DMZ.
    - PCI-DSS 1.3.3 Do not allow any direct routes inbound or outbound for traffic between the Internet and the cardholder data environment.
        - Disable DMZ hosting on the internet firewall.
    - PCI-DSS 1.3.4 Do not allow internal addresses to pass from the Internet into the DMZ.
        - Enable NAT (Network address translation) on your internet router.

- PCI-DSS 1.3.5 Restrict outbound traffic from the cardholder data environment to the Internet such that outbound traffic can only access IP addresses within the DMZ.
    - Enable NAT (Network address translation) on your internet router.
- PCI-DSS 1.3.6 Implement stateful inspection, also known as dynamic packet filtering. (That is, only ”established” connections are allowed into the network.)
    - Refer to the router manufacturer's documentation to enable dynamic packet filtering.
- PCI-DSS 1.3.7 Place the database in an internal network zone, segregated from the DMZ.
    - Enable NAT (Network address translation) on your internet router.
- PCI-DSS 1.3.8 Implement IP masquerading to prevent internal addresses from being translated and revealed on the Internet, using RFC 1918 address space. Use network address translation (NAT) technologies—for example, port address translation (PAT).
    - Enable NAT (Network address translation) on your internet router.

- PCI-DSS 1.4 which replaced PCI-DSS 1.3.9 Install personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization’s network.
    - Install personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization’s network directly or through remote desktop.

PA-DSS 11.2 Implement two-factor authentication for remote access to payment application.

- Use two-factor authentication (user ID and password and an additional authentication item such as a smart card, token or PIN) if the payment application may be accessed remotely.
    - CardWorks application contains no components that provide remote access.
    - WashGear does not support or endorse any specific remote access application.
    - Use of remote desktop applications to connect to the card processing environment requires the use of a token in addition to a user name and password to maintain PCI compliance.

Example:

- logmein.com combined with http://www.phonefactor.com

PA-DSS 11.3 Securely implement remote access software.

- Implement and use remote access software security features if remote access software is used to remotely access the payment application or payment environment.

If an application such as logmein is used for remote access to the PC, it is imperative that you configure strong encryption, and two factor authentication

Example:

- logmein.com combined with http://www.phonefactor.com

Examples of security features to enable:

- Change default settings in the remote access software
  - *Change default settings in the remote access software (for example, change default passwords and use unique passwords for each customer).* Allow connections only from specific (known) IP/MAC addresses.
- *Use strong authentication and complex passwords for logins according to PCI DSS Requirements 8.1, 8.3, and 8.5.8–8.5.15*
  - PA-DSS 8.1 Assign all users a unique ID before allowing them to access system components or cardholder data.
  - PA-DSS 8.3 Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties. 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.
  - PA-DSS 8.5.8 Do not use group, shared, or generic accounts and passwords.
  - PA-DSS **8.5.9** Change user passwords at least every 90 days.
  - PADSS **8.5.10** Require a minimum password length of at least seven characters.
  - PA-DSS **8.5.11** Use passwords containing both numeric and alphabetic characters.
  - PA-DSS **8.5.12** Do 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.
  - PA-DSS **8.5.13** Limit repeated access attempts by locking out the user ID after not more than six attempts.
  - PA-DSS **8.5.14** Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.
  - PA-DSS 8.5.15 If a session has been idle for more than 15 minutes, require the user to re-enter the password to reactivate the terminal.
- *Enable encrypted data transmission according to PCI DSS Requirement 4.1*
  - Use strong cryptography and security protocols such as SSL/TLS or IPSEC to safeguard sensitive cardholder data during transmission over open, public networks.

Examples of open, public networks that are in scope of the PCI DSS are:

- *The Internet,*
- *Wireless technologies,*
- *Global System for Mobile communications (GSM), and*
- *General Packet Radio Service (GPRS).*

- Enable account lockout after a certain number of failed attempts
    - Allow no more than 3 attempts before locking out remote login.
- Configure the system so a remote user must establish a VPN connection via a firewall before access is allowed.
    - If you need to use remote access software to access your system a VPN connection via a firewall should be implemented by a qualified IT professional.
- Enable the logging function.
    - Enable session logging within any remote access software that may be implemented on the system.
- **RESTRICT ACCESS TO CUSTOMER PASSWORDS TO AUTHORIZED RESELLER/INTEGRATOR PERSONNEL.**
    - **THIS IS A CRYTICAL SECURITY MEASURE**
    - If access to the remote systems requires the end-user (customer) to give access credentials (i.e. passwords) into the application these should be given only to known/authorized reseller/integrator personnel.
    - Never allow an unsolicited caller remote access to the card processing environment. If you are contacted by someone you don't personally recognize claiming to represent WashGear or a WashGear reseller requesting remote access or changes to your system, you must verify the identity of the caller by calling them back on the phone# you already possess and would normally use to contact them before proceeding.
    - Telnet or rlogin must never be used for administrative access.
- *Establish customer passwords according to PCI DSS Requirements 8.1, 8.2, 8.4, and 8.5.*
    - PA-DSS 8.1 Assign all users a unique ID before allowing them to access system components or cardholder data.
    - PA-DSS 8.2In addition to assigning a unique ID**,** employ at least one of the following methods to authenticate all users:
        - Password or passphrase
        - Two-factor authentication (for example, token devices, smart cards, biometrics, or public keys

PA-DSS 12.1 Secure transmissions of cardholder data over public networks.

- Implement and use SSL for secure cardholder data transmission over public networks, in accordance with PCI DSS Requirement 4.1
    - PCI-DSS 4.1 Use strong cryptography and security protocols such as SSL/TLS or IPSEC to safeguard sensitive cardholder data during transmission over open, public networks.

Examples of open, public networks that are in scope of the PCI DSS are:

- *The Internet,*
- *Wireless technologies,*
- *Global System for Mobile communications (GSM), and*
- *General Packet Radio Service (GPRS).*

- CardWorks communicates to the card processor using SSL security which fulfills this requirement.

PA-DSS 12.2 Encrypt cardholder data sent over end user Messaging technologies.

- Implement and use an encryption solution for if PANs can be sent with end-user messaging technologies.
    - CardWorks doesn't provide any way to access cardholder data and thus prevents the transmission of cardholder data over end user messaging technology.

PA-DSS 13.1 Encrypt non-console administrative access.

- Implement and use SSH, VPN, or SSL/TLS for encryption of any non-console administrative access to payment application or servers in cardholder data environment is critical in securing the card data environment.
    - CardWorks application contains no components that provide non-console administration.
    - WashGear does not support or endorse any specific remote access application.

If implementing non-console administrative access:

- Encrypt all non-console administrative access by implementing SSH, VPN, or SSL/TLS between the PC being administered and the PC where the Administrator is present.
- Strong encryption must be invoked before password is requested.
- Telnet or rlogin must never be used for administrative access.

Maintain an Information Security Program

In addition to the preceding security recommendations, a comprehensive approach to assessing and maintaining the security compliance of the payment application environment is necessary to protect the organization and sensitive cardholder data.

The following is a very basic plan every merchant/service provider should adopt in developing and implementing a security policy and program:

Read the PCI DSS in full and perform a security gap analysis. Identify any gaps between existing practices in your organization and those outlined by the PCI requirements.

Once the gaps are identified, determine the steps to close the gaps and protect cardholder data. Changes could mean adding new technologies to shore up firewall and perimeter controls, or increasing the logging and archiving procedures associated with transaction data.

Create an action plan for on-going compliance and assessment.

Implement, monitor and maintain the plan. Compliance is not a one-time event. Regardless of merchant or service provider level, all entities should complete annual self-assessments using the PCI Self Assessment Questionnaire.

Call in outside experts as needed.

- A list of Qualifies Security Assessors (QSA) is available at https://www.pcisecuritystandards.org/about/resources.shtml

Application System Configuration

Below are the operating systems and dependent application patch levels and configurations supported and tested for continued PCI DSS compliance.

- Microsoft Windows Vista or Windows XP with Service Pack 2. All latest updates and hot-fixes should be tested and applied.
- 1 GB of RAM minimum, 2 GB or higher will perform better
- 20 GB of available hard-disk space
- TCP/IP network connectivity on 2 ports.

Payment Application Initial Setup & Configuration

Application logging is required to maintain PCI compliance and disabling it in any way will result in non-compliance to PCI DSS.

CardWorks is designed to be PCI compliant. Compliance is not optional so there are no optional configuration settings that can be turned on or off relating to application logging or anything else that could prohibit PCI compliance within CardWorks.

- Application logging is required to maintain PCI compliance and disabling it in any way will result in non-compliance to PCI DSS.

    - CardWorks is designed to be PCI compliant. Compliance is not optional so there are no optional configuration settings that can be turned on or off relating to application logging or anything else that could prohibit PCI compliance within CardWorks.
- Set unique usernames and passwords for both administrators and basic users within CardWorks before accepting credit cards.
- When desired, the key encryption key (KEK) can be changed and data re-encrypted by an Admin user at any time. To do so Click Tools> Re-Encrypt

PCI related reminders for merchants

PCI-DSS 1.1.6 Requirement to review firewall and router rule sets at least every six months

PCI-DSS 8.5.5 Remove/disable inactive user accounts at least every 90 days.

PCI-DSS 8.5.9 Change user passwords at least every 90 days.

