MicroSale
Simple, Complete Food Service Systems

PA-DSS Implementation Guide

Version 2.2 – February 2014

Revision History

Changes	Approving Manager	Date
Added Revision History page	Steve Theroux	01/09/2014
MicroSale application version	Steve Theroux	01/09/2014
Supported operating systems	Steve Theroux	02/13/2014
Supported HW configurations	Steve Theroux	01/09/2014
Updated Review Summary	Steve Theroux	02/27/2014
Updated Executive Summary	Steve Theroux	01/09/2014
Updated Eraser web link	Steve Theroux	01/09/2014
Updated PCI DSS overview	Steve Theroux	01/13/2014
Updated network diagram	Steve Theroux	01/13/2014
Updated dataflow diagram	Steve Theroux	01/13/2014
Updated Introduction page	Steve Theroux	01/13/2014
New Encryption Key Management	Steve Theroux	01/16/2014
Updated Software Updates page	Steve Theroux	01/16/2014
Information Security Policy page	Steve Theroux	01/16/2014
Updated Encryption Key Management	Steve Theroux	02/27/2014
Updated Event Logging	Steve Theroux	02/04/2014
Secure Services and Protocols	Steve Theroux	02/27/2014
Supported HW configurations	Steve Theroux	05/21/2014

This document is the property of MicroSale: it contains information that is proprietary, confidential, or otherwise restricted from disclosure. If you are not an authorized recipient, please return this document to the above-named owner. Dissemination, distribution, copying or use of this document in whole or in part by anyone other than the intended recipient is strictly prohibited without prior written permission by MicroSale.

The purpose of this document is to educate resellers on the best methods for setting up and maintaining MicroSale in an environment that will securely protect the sensitive cardholder data used during payment processing based on the Data Security Standard established by the Payment Card Industry.

The primary goals are to reduce the chance of intrusion, increase the ability to detect intrusion, implement secure networking environments, and enhance system logging.

It is important to keep in mind that compliance is an ongoing process, not a one-time event.

Introduction

Systems which process payment transactions necessarily handle sensitive cardholder account information.

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 MicroSale 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 and software configurations and access control procedures.

The PA-DSS Validation is intended to ensure that MicroSale will help you achieve and maintain PCI Compliance with respect to how MicroSale 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 PA-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.

PCI DSS should be implemented into business-as-usual activities as part of your overall security strategy. This enables you to monitor the effectiveness of your security controls on an ongoing basis and maintain your PCI DSS compliant environment in between PCI DSS assessments.

PCI Data Security Standard High-Level Overview:

Build and Maintain a Secure Network and Systems

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

Protect Cardholder Data

3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

5. Protect all systems against malware and regularly update anti-virus software or programs
6. Develop and maintain secure systems and applications

Implement Strong Access Control Measures

7. Restrict access to cardholder data by business need-to-know
8. Identify and authenticate access to system components
9. Restrict physical access to 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 for all personnel

NOTICE

THE INFORMATION IN THIS DOCUMENT IS FOR INFORMATIONAL PURPOSES ONLY. MICROSALE MAKES NO REPRESENTATION OR WARRANTY AS TO THE ACCURACY OR THE COMPLETENESS OF THE INFORMATION CONTAINED HEREIN. YOU ACKNOWLEDGE AND AGREE THAT THIS INFORMATION IS PROVIDED TO YOU ON THE CONDITION THAT NEITHER MICROSALE NOR ANY OF ITS AFFILIATES OR REPRESENTATIVES WILL HAVE ANY LIABILITY IN RESPECT OF, OR AS A RESULT OF, THE USE OF THIS INFORMATION. IN ADDITION, YOU ACKNOWLEDGE AND AGREE THAT YOU ARE SOLELY RESPONSIBLE FOR MAKING YOUR OWN DECISIONS BASED ON THE INFORMATION PROVIDED HEREIN.

Nothing herein shall be construed as limiting or reducing your obligations to comply with any applicable laws, regulations or industry standards relating to security or otherwise including, but not limited to, PA-DSS and DSS.

The retailer may undertake activities that may affect compliance. For this reason, MicroSale is required to be specific to only the standard software provided by us.

This document describes the steps that must be followed in order for your MicroSale installations to comply with Payment Application – Data Security Standards (PA-DSS).

The information in this document is based on PCI Security Standards Council Payment Application Data Security Standards program (ver 2.0 dated October 2010). MicroSale instructs and advises its customers to deploy MicroSale applications in a manner that adheres to the PCI Data Security Standard (v2.0). Subsequent to this, best practices and hardening methods, such as those referenced by the Center for Internet Security (CIS) and their various “Benchmarks”, should be followed in order to enhance system logging, reduce the chance of intrusion and increase the ability to detect intrusion, as well as other general recommendations to secure networking environments. Such methods include, but are not limited to, enabling operating system auditing subsystems, system logging of individual servers to a centralized logging server, the disabling of infrequently-used or frequently vulnerable networking protocols and the implementation of certificate-based protocols for access to servers by users and vendors.

If you do not follow the guidelines outlined in this document, your MicroSale installations will not be PCI PA-DSS compliant.

Application Summary

This document supports the following application version:

MicroSale version 9.0

Below are the operating systems and dependent application patch levels and configurations supported and tested for continued PA-DSS compliance:

- Windows Server 2008 with Service Pack 2, Windows 7 Professional with Service Pack 1, Windows Embedded POSReady 7, Windows Embedded POSReady 2009 with Service Pack 3.
- 1.8 GHz dual-core CPU minimum; 2.0 GHz dual-core or faster recommended
- 1.0 GB of RAM minimum; 2.0 GB or more recommended
- 10.0 GB of available hard disk space
- TCP/IP network connectivity
- Internet Explorer 8 or higher required; Internet Explorer 9 recommended
- SQL Server 2005, SQL Server 2008, or SQL Server Express Edition

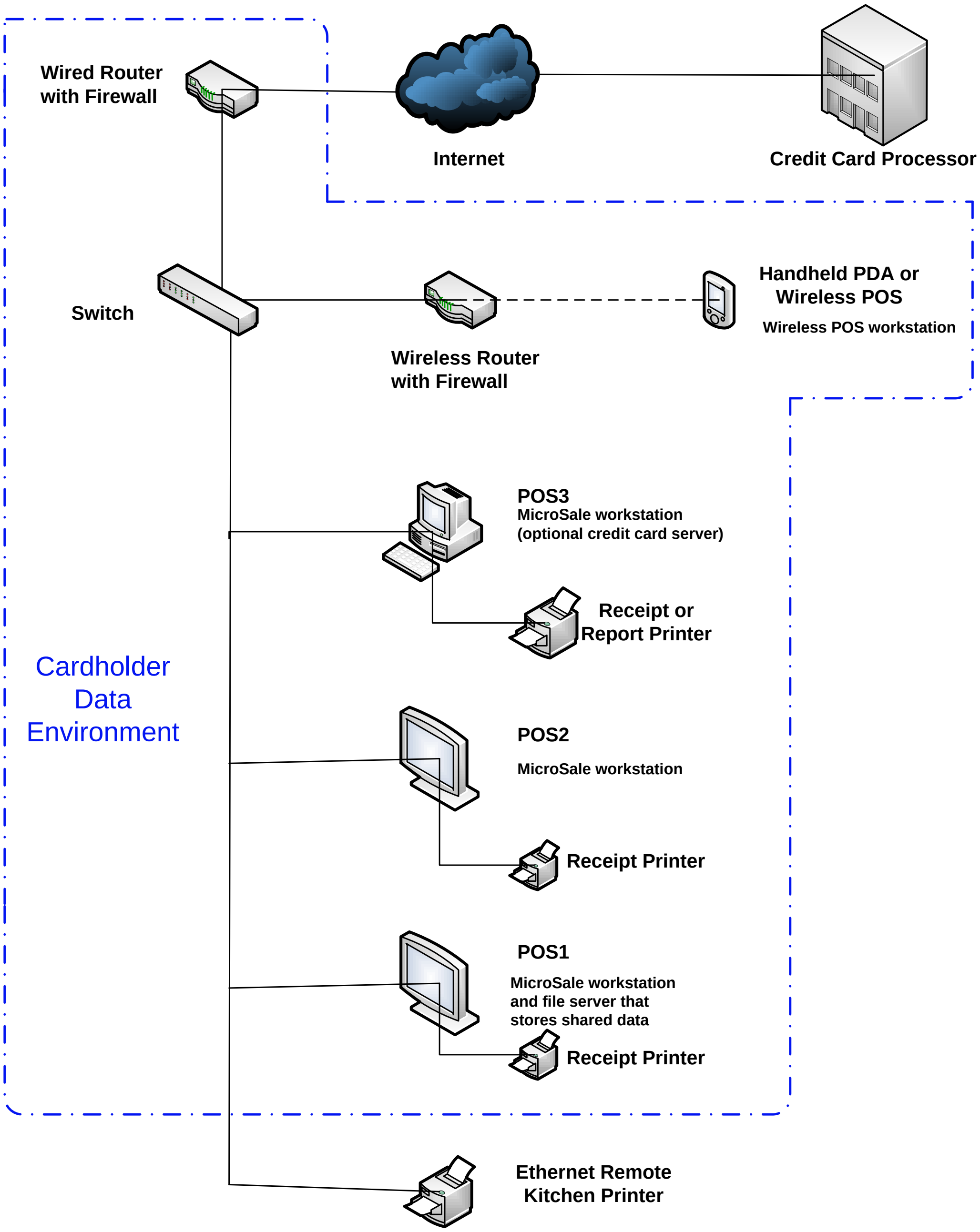
All latest updates, service packs, and hot-fixes should be tested and applied.

PCI PA-DSS Payment Application Environment Requirements

Network Segmentation

The PCI DSS requires that firewall services be used (with NAT or PAT) to segment network segments into logical security domains based on the environmental needs for internet access. Traditionally, this corresponds to the creation of at least a DMZ and a trusted network segment where only authorized, business-justified traffic from the DMZ is allowed to connect to the trusted segment. No direct incoming internet traffic to the trusted application environment can be allowed. Never store cardholder data on Internet-accessible systems (e.g., web server and database server must not be on same server.) Additionally, outbound internet access from the trusted segment must be limited to required and justified ports and services.

A simplified high-level diagram of an expected network configuration for a web-based payment application environment is included below:


Wired Router with Firewall
Internet
Credit Card Processor
Switch
Wireless Router with Firewall
Handheld PDA or Wireless POS
Wireless POS workstation
POS3
MicroSale workstation (optional credit card server)
Receipt or Report Printer
Cardholder Data Environment
POS2
MicroSale workstation
Receipt Printer
POS1
MicroSale workstation and file server that stores shared data
Receipt Printer
Ethernet Remote Kitchen Printer

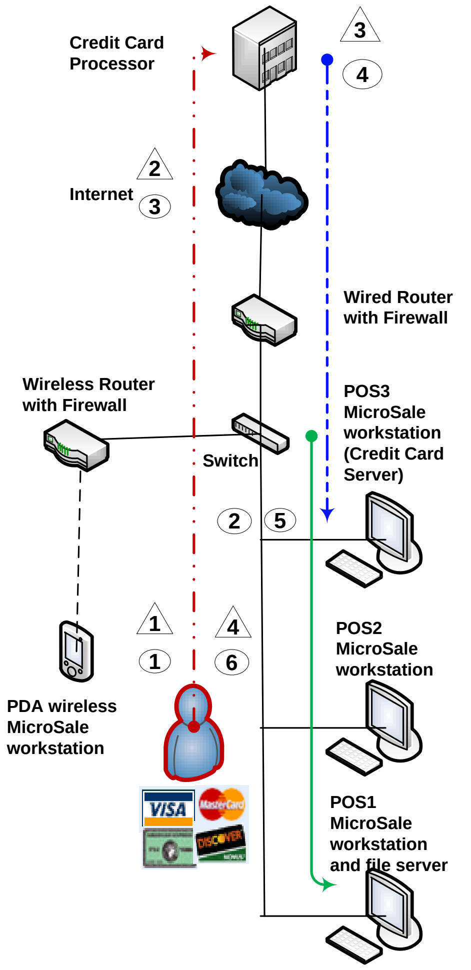
Data Transport Encryption

The PCI DSS requires the use of strong cryptography and encryption techniques with at least 128-bit encryption strength (either at the transport layer with SSL or IPSEC; or at the data layer with algorithms such as RSA or Triple-DES) to safeguard sensitive cardholder data during transmission over public networks (this includes the Internet and Internet-accessible DMZ network segments).

MicroSale does not allow or facilitate the sending of PANs via any end user messaging technology (such as email, instant messaging, chat, etc.).

Dataflow Diagram

The following diagram illustrates the flow of encrypted data in a MicroSale system:


Credit Card Processor
3
4
2
Internet
3
Wired Router with Firewall
Wireless Router with Firewall
Switch
POS3 MicroSale workstation (Credit Card Server)
2
5
1
1
4
6
POS2 MicroSale workstation
PDA wireless MicroSale workstation
POS1 MicroSale workstation and file server

NETePay Configuration:

1 - Card data is captured and encrypted at the MicroSale workstation.

2 - MicroSale sends the request to the Credit Card Server running the Credit Card Server Software (NETePay).

3 - NETePay sends the request across the Internet to the Processor.

4 - Processor returns the response across the Internet to NETePay.

5 - NETePay returns the authorization to the MicroSale workstation where the request originated.

6 - MicroSale workstation prints the authorization slip for signature capture and stores the transaction details in the encrypted credit card database on the file server.

Direct Connection Configuration (e.g., Mercury):

1 - Card data is captured and encrypted at the MicroSale workstation.

2 - MicroSale sends the request across the Internet to the Processor.

3 - Processor returns the response to the MicroSale workstation where the request originated.

4 - MicroSale workstation prints the authorization slip for signature capture and stores the transaction details in the encrypted credit card database on the file server.

Authorization request is sent from a POS terminal through the local network across the Internet to the processor.

Response is returned to the POS terminal that sent the request, and the authorization slip prints for signature capture.

Approved transactions are stored on the file server until the batch is settled during the Daily Closeout process.

Access Control

The PCI DSS requires that access to all systems in the payment processing environment be protected through use of unique users and complex passwords. Unique user accounts indicate that every account used is associated with an individual user and/or process with no use of shared, group, or generic accounts used by more than one user or process. Additionally any default accounts provided with operating systems, databases and/or devices should be removed/disabled/renamed as possible, or at least should have PCI DSS compliant complex passwords assigned to them and should not be used. Examples of default administrator accounts include “administrator” (Windows systems), “sa” (SQL/MSDE), and “root” (UNIX/Linux).

The PCI standard requires the following password complexity for *secure authentication*:

- Passwords must be at least 7 characters
- Passwords must include both numeric and alphabetic characters
- Passwords must be changed at least every 90 days
- New passwords can not be the same as the last 4 passwords used

PCI user account requirements for *secure authentication* beyond user account uniqueness and password complexity are listed below:

- If an incorrect password is provided 6 times the account should be locked out
- Account lock out duration should be at least 30 min. (or until an Administrator resets it)
- Sessions idle for more than 15 minutes should require re-entry of username and password to reactivate the session.

These user account and password criteria must also be applied to any applications or databases included in payment processing. Furthermore, user accounts with administrative privileges should not be used for application logins. MicroSale, as tested in our PA-DSS audit, meets or exceeds these requirements.

Changing these settings for unique user ID's and secure authentication will result in non-compliance with the PCI-DSS.

Remote Access

Remote access is the ability to connect and interact with a remote network or computer as if you were directly connected to or using that remote network device or computer. The best policy to ensure the safest and most secure environment for payment processing is to not allow remote connections to merchant sites. However, there may be times when you must connect remotely to a client site.

The PCI standard requires that if employees, administrators, or vendors are granted remote access to the payment processing environment; access should be authenticated using a two-factor authentication mechanism (username/ password and an additional authentication item such as a token or certificate).

In the case of vendor remote access accounts, in addition to the standard access controls, vendor accounts should only be active while access is required to provide service. Access rights should include only the access rights required for the service rendered, and should be robustly audited.

If users and hosts within the payment application environment need to use third-party remote access software such as VnC, Remote Desktop (RDP)/Terminal Server, PCAnywhere, etc. to access other hosts within the payment processing environment, special care must be taken.

In order to be compliant, every such session must be encrypted with at least 128-bit encryption (in addition to satisfying the requirement for two-factor authentication required for users connecting from outside the payment processing environment). For RDP/Terminal Services this means using the high encryption setting on the server, and for PCAnywhere it means using symmetric or public key options for encryption. The standard PCI user account and password requirements will apply to these access methods as well.

When requesting support from a vendor, reseller, or integrator, customers are advised to take the following precautions: ensure that any such remote connection is initiated by an outbound connection that does not require firewall port enablement, and the individual requesting support must monitor the system environment while the remote connection is active.

Furthermore, be sure to implement the following security features:

- Change all default settings when installing remote access or remote control software including usernames and passwords.
- Use unique passwords for each customer.
- Allow connections from only specific (known) MAC or IP addresses
- Use strong authentication or complex passwords for logins
- Enable encrypted data transmission
- Enable account lockout after a certain number of failed login attempts
- Configure the system so a remote user must establish a Virtual Private Network (VPN) connection via a firewall before access is allowed.
- Enable logging functions.
- Restrict access to customer passwords to authorized personnel only.
- Implement **two-factor authentication** for remote access to the network requiring unique usernames, strong passwords, and an additional item such as a certificate, token, or VPN with individual certificates.

When considering solutions, the following principles must be addressed to ensure that the solution provides needed controls without enabling "full" remote access:

- Ensure that remote connectivity can be traced to a specific service request (to identify the support technicians involved and the customer requesting support).
- Ensure that the solution does not allow "on demand" or "always on" access. Remote access must be turned on by the customer requesting support only when needed, and access must be disabled as soon as the support task is resolved.
- Ensure the solution uses robust (at least 128 bit) encryption.
- Ensure that the solution does not allow for the exchange of credentials.
- Mandate that the customer environment must be monitored while access is enabled.
- Ensure that the connection is enabled by an outbound connection that does not require firewall port enablement.

Non-Console Administration

Users and hosts within the payment application environment may need to use third-party remote access software such as Remote Desktop (RDP)/Terminal Server, pcAnywhere, VnC, etc. to access other hosts within the payment processing environment. However, to be compliant, every such session must be encrypted with at least 128-bit encryption using technologies such as SSH, VPN, or SSL/TLS in addition to satisfying the requirement for two-factor authentication required for users connecting from outside the payment processing environment. For RDP/Terminal Services this means using the high encryption setting on the server, and for pcAnywhere it means using symmetric or public key options for encryption. The PCI user account and password requirements will apply to these access methods as well.

Definition of Two-Factor Authentication

In identifying and authorizing users for access, you must use two of the three authentication methods below to constitute valid two-factor authentication:

- Something you know, such as the User ID/Password combination
- Something you have, such as a Digital Certificate or RSA token
- Something you are, such as a Biometric ID mechanism.

Note that two different sets of a single method (e.g., two User ID/Password combinations) do not create a valid two-factor authentication scenario.

It is also important to note that both methods of authentication must uniquely identify a specific person or user, not a group of people or users.

Traditional scenarios supported and expected for two-factor remote access include the use of User ID/Password at the network or computer level in combination with a Certificate or RSA SecureID used to authorize an encrypted VPN connection.

Wireless Access Control

MicroSale does support wireless technologies, and the following guidelines for secure wireless settings must be followed:

Perimeter firewalls must be installed between any wireless networks and systems that store cardholder data, and these firewalls must deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.

Furthermore:

- All wireless networks must implement strong encryption (e.g. AES)
- Encryption keys must be changed from the default at installation and must also be changed anytime anyone with knowledge of the keys leaves the company or changes positions
- Default SNMP community strings on wireless devices must be changed
- Default passwords/passphrases on access points must be changed
- Firmware on wireless devices must be updated to support strong encryption for authentication and transmission over wireless networks (e.g., WPA/WPA2)
- Industry best practices must be used to implement strong encryption for the following over the wireless network in the cardholder data environment:
    - ◊ Transmission of cardholder data
    - ◊ Transmission of authentication data
- The use of WEP for wireless encryption in payment application environments is now prohibited as WEP is no longer PCI-compliant

MicroSale Configuration

This document provides specific installation, configuration, and ongoing management best practices for using MicroSale as a PA-DSS validated application operating in a PCI-Compliant environment. Step-by-step instructions for setting up MicroSale terminals are provided in the ***M$ PC Setup Instructions.pdf*** document. Setup instructions for the SMC wireless router can be found in the ***Wireless Router Setup for SMCWBR14S-N3.pdf*** document, and setup instructions for the Widefly wireless PDA terminal are in the ***WF35 Configuration for Micro$ale.pdf*** document.

Credit Card Merchant Account Setup

Credit card batch settlement must be initiated daily from the end user site. Host-initiated and timed batch settlements are not supported by MicroSale. Client accounts must also be setup to use Merchant Category Code 5812 or 5814 for restaurants.

Windows Operating System User Accounts

As previously discussed, do not use the default Windows *Administrator* or *Guest* accounts. Set new complex passwords/ passphrases for both, and disable the Guest account. Then setup new accounts using unique usernames and complex passwords/ passphrases.

Anti-Virus Protection

Install and regularly update anti-virus software, and run regular scans on each system. If virus activity is detected, disconnect that system from the network until it is clean and free of all virus activity.

Router and Firewall Protection

A network router with firewall services must be used to protect all systems connected to the Internet. Change the default password for the router when it is installed, and change it again at regular intervals not longer than 3 months. Use unique passwords for each client, and restrict access to these passwords to authorized personnel only. Do not enable any port forwarding for remote connections or unnecessary services.

Secure Services and Protocols

The payment application must only use/ require necessary and secure services, protocols, daemons, components, and dependent software and hardware for any functionality of the payment application, by default, “out of the box”. MicroSale does not require NetBIOS, Telnet, FTP, or other such services.

Remove all Test Accounts, Test Payment Card Numbers, and Test Charges

Ensure all test accounts, test card numbers, and test charges are removed prior to processing live data. Ensure all test accounts, test card numbers, and test charges are also removed before releasing or implementing software updates or patches.

Encryption Key Management

Encryption keys for PAN data stored or transmitted by MicroSale are created using a random number generator to create a 128-bit key. A new encryption key is created every day after the credit card batch settlement is confirmed during the Daily Close Out process. The encryption key can also be rotated on demand using the **Clear Batch** Administrator function in MicroSale if there is suspicion or evidence of an encryption key compromise. The encryption key is not stored or distributed, so there is no key custodian.

When a customer’s PAN and card expiration date are stored for recurrent charges (for regular customers with house accounts and regular call-in order customers), each entry is uniquely encrypted such that if one record is compromised, no other record can be decrypted.

Storage and Handling of Sensitive Cardholder Data

MicroSale uses SSL for secure transmission of cardholder data across the Internet. MicroSale does NOT support the transmission of cardholder data via email. Customers should NEVER send unencrypted cardholder data via email. MicroSale encrypts sensitive data while stored, but there are additional security measures that must be taken to ensure data security. Customers should develop a data retention and disposal policy that facilitates purging cardholder data after a defined period of time to so that such data is only stored for the amount of time necessary for business, legal, and regulatory purposes and so that such data is purged upon the expiration of that defined retention time. Support technicians must follow additional guidelines to insure data security: only collect sensitive data when necessary for a specific issue, collect only the specific data that is necessary for the issue at hand, store that data in a known, secure location with limited access, and securely delete all sensitive data immediately after use. Use trouble tickets or CRM software as an audit trail to document the safe handling of sensitive cardholder data by the specific personnel involved.

Secure deletion involves removing sensitive data by overwriting it several times with carefully selected patterns using a utility such as Eraser (http://eraser.heidi.ie/) so that such data is completely irrecoverable. Eraser is free software, and its source code is released under GNU General Public License.

Purging of Cardholder Data

Cardholder data should not be stored any longer than is necessary for business purposes. You should create a documented policy stating how long to store this data before purging it from the system, and be sure to implement the policy so that such data is purged after this set retention period. For example, your policy could state to purge stored cardholder data for all customers who have not placed an order for 6 months. The following guidelines must be followed when dealing with cardholder data (PAN alone or with any of the following: expiration date, cardholder name, or service code):

- ➢ A customer defined retention period must be defined with a business justification.
- ➢ Cardholder data exceeding the customer-defined retention period must be purged.
- ➢ Here are the locations of the cardholder data you must purge:
    - ◊ Call In Orders.mdb or CALL IN ORDERSSQL.mdf
        - - Customer Data table
    - ◊ Scan.mdb or HOUSE ACCOUNTS.mdf
        - - General Data table

To purge the cardholder data you must run the *Remove Inactive Credit Cards* Administrator function in MicroSale. Go to the **Manager Menu**, then **Gift Certificate House Account**, then **Reports / Utilities**, and click ***Remove Inactive Credit Cards***. Login with your Administrator Account username and password, and enter the number of days an account has been inactive to be included in this purge session based on your store policy as defined above. This will purge stored credit card data for both Call In Orders and House Accounts. This should be performed at least quarterly.

MicroSale Software Updates and Secure Delivery

We are committed to developing, testing, and releasing patches for any known vulnerabilities within 30 days after discovery of the vulnerability.

We strive to correct software bugs as soon as they are discovered and make patches available within one week, whenever possible. MicroSale dealers will be notified by phone and/ or email when a necessary patch is made available, and the patch will be downloaded by them from a secure read-only ftp site, transferred directly to them via secure remote access, or an upgrade CD will be sent to them if secure remote access is not available. MicroSale dealers are then responsible for going onsite or connecting remotely to upgrade their customers. MicroSale direct end users will be notified by phone or email when a necessary patch is available, and the update will be transferred directly to the customer site and installed remotely, or an upgrade CD will be sent if secure remote access is not available. Typically, resellers and merchants are expected to respond quickly and encouraged to install available patches within 30 days.

Remote delivery of software updates is only supported through remote control software solutions. When implementing MicroSale updates remotely, technicians must apply the same security and logging procedures discussed above. In addition, when connecting via dial-up for Remote Access using a modem and phone line, ensure that the customer only connects or turns on the modem when it is needed and that the modem is turned off or disconnected immediately after the update is complete. Customers must monitor their POS system environment the entire time that a technician is remotely connected to it, and Support Logs or Trouble Tickets must be completed that identify the support technicians involved and the customers who enabled the remote access and monitored the system environment during the remote access session.

Remove Historical Authentication Data and Cryptographic Material

An important part of the MicroSale upgrade process is removing any and all historical sensitive authentication data and cryptographic key material that may be leftover from credit card processing using previous versions of MicroSale. Since historic cardholder data cannot be re-encrypted, such removal is absolutely necessary for PCI compliance.
All MicroSale files from past and current versions are stored in the directory **C:\Program Files\Micro$ale** or **C:\Program Files (x86)\Micro$ale\** or the Microsoft SQL Server **Data** directory in use**.**

Before running live credit card charges through the upgraded system, run the **Legacy Clean** Removal Tool in the ***DatabaseUtility.exe*** program that is in **C:\Program Files\Micro$ale** or **C:\Program Files (x86)\Micro$ale\**, or manually search for and securely delete all of the following files:

> **Approvals.mdb, Approvals.bak, AppprovalsSQL.ldf, AppprovalsSQL.mdf,**
> **Last Batch.mdb, Last Batch.bak, DTBatch.mdb, DTBatch.bak, CCEncrypter.exe,**
> ***SitenameAddress*.71x, *SitenameAddress*.80x, *SitenameAddress*.90x**
> (where ***SitenameAddress*** is the merchant business name and address)
> ***Terminalname* Batch.mdb, *Terminalname* Batch.bak**
> (where ***Terminalname*** is the Windows network name of a POS terminal)

MicroSale version 9 does not and cannot store card validation values or codes, PINs, or PIN block data. Securely deleting the files listed above will ensure that all magnetic stripe data stored by previous versions has been removed and that all cryptographic key materials from previous versions have also been deleted.

Ensure that the original and all copies of these files are *securely* deleted. Such removal is absolutely necessary for PCI compliance.

MicroSale Administrative Accounts

MicroSale requires unique usernames and complex passwords for all Administrative access and for all access to cardholder data in addition to the standard login with an ID number or magnetic card. Unique usernames with secure authentication passwords are necessary to identify the individual responsible for changes or other actions that may result in non-compliance.

Note: These password controls are not intended to apply to employees who only have access to one card number at a time to facilitate a single transaction. These controls are applicable for access by employees with administrative capabilities, for access to servers with cardholder data, and for access controlled by the application.

Administrative functions include changing the MicroSale configuration, changing credit card processing settings, changing employee administrative privileges, clearing credit card batches, viewing system logs, and exiting from MicroSale to Windows.

Properly Train and Monitor Administrative Personnel

It is your responsibility to institute proper personnel management techniques for allowing Administrative user access to cardholder data, site data, etc. In most systems, a security breach is the result of unethical personnel, so pay special attention to whom you trust with Administrative access to your site and cardholder data, especially fully decrypted and unmasked payment information.

Event Logging

MicroSale has PA-DSS compliant logging enabled by default. This logging is not configurable and may not be disabled. MicroSale logs all functions involving access to cardholder data and all functions requiring Administrative access including viewing the logs themselves. These logs are archived to a central location on the file server once per week during the Weekly Closeout process. **Attempting to disable or subvert these logging functions will result in non-compliance with the PCI DSS.**

The main purposes for logging these events are to prevent or detect unauthorized access and to provide good forensic evidence to reconstruct what occurred in the event of a compromise.

Maintain an Information Security Policy/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. Visa has published a Qualified Security Assessor List of companies that can conduct on-site PCI-compliance audits for Level 1 Merchants, MasterCard has published a Compliant Security Vendor List of approved scanning vendors, and many credit card processors also partner with qualified security assessors to offer regular (quarterly) scanning services for their customers at a discounted rate, some with insurance against the audit costs and potential fines in the event that a data security breach occurs.

Review Summary

This Implementation Guide and accompanying **PCI Training Module** are to be reviewed and updated at least annually, when new software versions are released, and when there are changes to the PA-DSS requirements by the Payment Card Industry. This Implementation Guide and subsequent updates will be distributed to new dealers and resellers during their training session. It is also included on the MicroSale installation media and is available for download from our website or ftp site.

M$ PA-DSS Implementation Guide	**M$ PCI Training Module**
Date last reviewed: 08/15/2014	Date last reviewed: 08/15/2014
Reviewed By: Steve Theroux	Reviewed By: Steve Theroux
Date last modified: 05/21/2014	Date last modified: 05/21/2014
Modified By: Steve Theroux	Modified By: Steve Theroux

Executive Summary

MicroSale version 9.0 has been PA-DSS (Payment Application Data Security Standard) certified, with PA-DSS Version 2.0. For the PA-DSS assessment, we worked with the following PCI SSC approved Payment Application Qualified Security Assessor (PAQSA):

Trustwave
70 West Madison Street, Suite 1050
Chicago, IL 60602
www.trustwave.com

More Information

The following documents provide additional detail surrounding the Payment Card Industry Security Standards Council and related security programs (PA-DSS, PCI DSS, etc.):

- Payment Applications Data Security Standard (PA-DSS)
  https://www.pcisecuritystandards.org/security_standards/pa_dss.shtml

- Payment Card Industry Data Security Standard (PCI DSS)
  https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

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

- Your credit card processor may also offer educational resources and assistance with quarterly network scans and annual self-assessment questionnaires (SAQ)

MicroSale

Simple, Complete Food Service Systems

Reseller PCI Training Confirmation Receipt

I have read the MicroSale *PA-DSS Implementation Guide*, and I have reviewed the standards and policies set forth by the Payment Card Industry Security Standards Council (PCI SSC), namely the Payment Card Industry Data Security Standard.

I have been trained by MicroSale's staff, and I understand how to set up and maintain MicroSale in an environment that will securely protect the sensitive cardholder data used during payment processing based on these standards set forth by the Payment Card Industry Security Standards Council.

I further understand that PCI-compliance entails implementing a PCI-compliant environment for payment processing, not just upgrading the version of MicroSale.

As a MicroSale Reseller, I understand that it is my responsibility to educate my customers and staff on the best practices for implementing and maintaining a MicroSale point-of-sale system in an environment that will keep the sensitive cardholder data used during payment processing safe and secure.

______________________________ Signature	______________________________ Date
______________________________ Printed Name	______________________________ Company Name
______________________________ Position or Title	______________________________ Street Address
______________________________ Trainer Signature	______________________________ City, State, ZIP

MicroSale
Simple, Complete Food Service Systems

End User PCI Training Confirmation Receipt

I have seen the MicroSale PCI Training Module, I have been trained by my MicroSale dealer, and I understand how to operate and maintain MicroSale in an environment that will securely protect the sensitive cardholder data used during payment processing based on the Data Security Standard (DSS) set forth by the Payment Card Industry Security Standards Council (PCI SSC).

I also understand that PCI-compliance entails implementing a PCI-compliant environment for payment processing, not just upgrading the version of MicroSale.

As a MicroSale End User, I understand that I am ultimately responsible for protecting the cardholder data processed through my point-of-sale system and that it is my responsibility to educate my staff on the best practices for implementing and maintaining my point-of-sale system in an environment that will keep the cardholder data used during payment processing safe and secure.

Signature   Date

Printed Name   Company Name

Position or Title   Street Address

Trainer Signature   City, State, ZIP

MicroSale
Simple, Complete Food Service Systems

End User PCI Opt-Out Confirmation Receipt

I understand that my point-of-sale system does not currently meet all of the requirements for PCI-compliance based on the PCI Data Security Standard.

I have been advised by my point-of-sale dealer or software provider as to the requirements necessary for PCI-compliance.

I further understand that I am ultimately responsible for protecting the sensitive cardholder data processed through my point-of-sale system.

Signature

Date

Printed Name

Company Name

Position or Title

Street Address

Trainer Signature

City, State, ZIP