micros®

RES Version 3.2 Service Pack 7 Hotfix 5 with Transaction Vault Electronic Payment Driver Version 4.3 PCI Data Security Standard Adherence

General Information

About This Document

This document is intended as a quick reference guide to provide you with information concerning MICROS' adherence to the Visa USA PCI Data Security Standard concerning PABP compliance. This document relates specifically to the MICROS Restaurant Enterprise Solutions (RES) Version 3.2 Service Pack 7 Hotfix 5 with Transaction Vault Electronic Payment Driver Version 4.3 installed for electronic payment processing.

About CISP Compliance

When customers offer their bankcard at the point of sale, over the Internet, on the phone, or through the mail, they want assurance that their account information is safe. That's why Visa USA has instituted the Cardholder Information Security Program (CISP). Mandated since June 2001, the program is intended to protect Visa cardholder data—wherever it resides—ensuring that members, merchants, and service providers maintain the highest information security standard[1].

For more detailed information concerning CISP compliance, please refer to the Visa USA CISP website, <*http://usa.visa.com/download/business/accepting_visa/ops_risk_management/cisp.html*>.

1. Reprinted from "Cardholder Information Security Policy", <*http://usa.visa.com/download/business/accepting_visa/ops_risk_management/cisp.html*>.

About The PCI Data Security Standard

CISP compliance is required of all merchants and service providers that store, process, or transmit Visa cardholder data. The program applies to all payment channels, including retail (brick-and-mortar), mail/telephone order, and ecommerce. To achieve compliance with CISP, merchants and service providers must adhere to the Payment Card Industry (PCI) Data Security Standard, which offers a single approach to safeguarding sensitive data for all card brands. This Standard is a result of a collaboration between Visa® and MasterCard® and is designed to create common industry security requirements, incorporating the CISP requirements. Other card companies operating in the U.S. have also endorsed the PCI Data Security Standard within their respective programs.

Using the PCI Data Security Standard as its framework, CISP provides the tools and measurements needed to protect against cardholder data exposure and compromise across the entire payment industry. The PCI Data Security Standard, seen below, consists of twelve basic requirements supported by more detailed sub-requirements:[2]

*The **Payment Card Industry (PCI) Data Security Standard** is a result of a collaboration between Visa and MasterCard to create common industry security requirements. Other card companies operating in the U.S. have also endorsed the Standard within their respective programs. These 12 requirements are the foundation of Visa's CISP.*

PCI Data Security Standard

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 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

2. Reprinted from "CISP_overview.pdf", <*http://usa.visa.com/download/business/accepting_visa/support_center/cisp_overview.pdf?it=c|/business/accepting_visa/ops_risk_management/cisp%2Ehtml|CISP%20Overview*>.

Who Should be Reading this Document

This document is intended for the following audiences:

MICROS Installers/Programmers

MICROS Dealers

MICROS Customer Service

MICROS Training Personnel

MIS Personnel

MICROS Customers

What the Reader Should Already Know

This document assumes that you have the following knowledge or expertise:

Operational understanding of PCs

Understanding of basic network concepts

Experience with Microsoft Windows 2000

Familiarity with the MICROS RES Software

Familiarity with operating MICROS peripheral devices

RES Version 3.2 Service Pack 7 Hotfix 5 with Transaction Vault Version 4.3 and the PCI Data Security Standard

PCI Data Security Standard

While MICROS Systems Inc. (MICROS) recognizes the importance of upholding card member security and data integrity, certain parameters of the PCI Data Security Standard and CISP compliance are the sole responsibility of the client. This section contains a description of the 12 points of The PCI Data Security Standard and discusses how the Restaurant Enterprise Solution (RES) Version 3.2 Service Pack 7 Hotfix 5 with Transaction Vault Version 4.3 software adheres to it.

For a complete description of the PCI Data Security Standard, please consult Visa USA's website "Cardholder Information Security Plan" found at <*http://usa.visa.com//download/business/accepting_visa/ops_risk_management/cisp.html*>.

Document Conventions

This document is organized by each of the 12 basic requirements outlined in the PCI Data Security Standard. For each requirement, there is a MICROS Development response or recommendation that applies to RES Version 4.1 software.

Build and Maintain a Secure Network

1. Install and maintain a firewall configuration to protect data

Firewalls are computer devices that control computer traffic allowed into a company's network from outside, as well as traffic into more sensitive areas within a company's internal network. All systems need to be protected from unauthorized access from the Internet, whether for e-commerce, employees' Internet-based access via desktop browsers, or employees' email 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[3]

In accordance with the Visa USA PCI Data Security Standard, MICROS recommends every site install and maintain a firewall configuration to protect data. Configure your network so that databases and wireless access points always reside behind a firewall and have no direct access to the Internet.

3. "PCI Security Audit Procedures", p. 5, V. 1.0, December 15, 2004. <*http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_tools_faq.htm*>

To make sure your firewall configuration is set up in compliance with Step 1 of the PCI Data Security Standard, "Install and maintain a firewall configuration to protect data", please consult Visa USA's website, "Cardholder Information Security Policy", <*http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html*>.

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 are easily determined via public information[4]

RES 3.2 SP 7 HF 5 with Transaction Vault requires several default database users be installed with the system and remain unchanged by the site. These users' passwords are not published by MICROS and should not be changed by the site. No database user has access to unencrypted credit card information. Listed below are the database users that are required to run the system and need to remain untouched.

List of Database Users

DBA	REPORTS
MICROS	REPORTUSER
CAEDC	SETUP
DBSRPC	SYSCFG
EOSAPPS	CUSTOM
ESD	EMPREPL
GSSCFG	INSTALLER
GSSSERVER	MANAGER
KDSSERVER	SUPPORT
PROCEDURES	

4. "PCI Security Audit Procedures", p. 10, V. 1.0, December 15, 2004. <*http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_tools_faq.html*>.

RES 3.2 SP 7 HF 5 with Transaction Vault requires a default operating system user be installed with the system and remain unchanged by the site. The users name is microssvc.

All other operating system users passwords should be changed on a regular basis by the site following PCI standards for password management.

All application users passwords should be changed on a regular basis by the site following PCI guidelines for password management.

For all other system components, including operating system, network devices, and access points, MICROS recommends changing all vendor-supplied default passwords to a complex password.

For more information on Step 2 of The PCI Data Security Standard, "Do not use vendor-supplied defaults for system passwords and other security parameters", please consult Visa USA's website, "Cardholder Information Security Policy", *<http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html>*.

Protect Cardholder Data

3. Protect stored data

Encryption is the ultimate protection mechanism because even if someone breaks through all other protection mechanisms and gains access to encrypted data, they will not be able to read the data without further breaking the encryption. This is an illustration of the defense in depth principle[5]

MICROS interprets this requirement to mean the following:

1. **Do not store complete track data subsequent to obtaining authorization.**

   Under no circumstances will RES 3.2 SP7 HF 5 with Transaction Vault store sensitive track data.

2. **Do not allow access to full credit card numbers in the store. Also, mask or encrypt credit card numbers wherever they are printed or stored.**

   With the release of RES 3.2 SP 7 HF 5 with Transaction Vault, the existing masking option bits have been enhanced to provide masking

5. "PCI Security Audit Procedures", p. 13, V. 1.0, December 15, 2004. *<http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_tools_faq.html>*

of a credit card number (all but the last four digits) and its expiration date (all digits) from any printout or display device where it might be viewed by an unauthorized person. This includes workstation displays, hardware devices (pole displays, hand-helds, Pin Pads), as well as system reports, journals, and log entries. The following POS Configurator option bits apply:

Sales | Tender/Media | CC Tender| Mask Credit Card Number

Sales | Tender/Media | CC Tender| Mask Expiration Date

Sales | Tender/Media | CC Tender| Mask Cardholder Name - When this option is enabled, the cardholder name is not saved to the database.

MICROS recommends selecting these three option bits for all credit card tenders.

For more information on Step 3 of The PCI Data Security Standard, "Protect stored data", please consult Visa USA's website, "Cardholder Information Security Policy", <*http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html*>.

4. Encrypt transmission of cardholder data and sensitive information across public networks

Sensitive information must be encrypted during transmission over the Internet, because it is easy and common for a hacker to intercept and/or divert data while in transit[6]

When transmitting cardholder data over a public network or the Internet, *always* use SSL version 3.0, and when transmitting wirelessly, *always* use the highest level of encryption available.

RES 3.2 SP7 HF 5 supports protocol-level encryption features of the operating system and networking equipment such as WEP (Wired Equivalency Protocol), IPSEC (IP Security) and WPA (Wi-Fi Protected Access).

Sensitive data stored in the MICROS database is encrypted via a strong encryption algorithm (Triple-DES). Sensitive data is defined as the cardholder account number, expiration date and cardholder name. The encryption key is unique per merchant and can be rotated by end-user.

For more information on Step 4 of The PCI Data Security Standard, "Encrypt transmission of cardholder data and sensitive information across public networks", please consult Visa USA's website, "Cardholder Information Security Policy", <*htttp://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html*>.

6. "PCI Security Audit Procedures", p. 18, V. 1.0, December 15, 2004. <*http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_tools_faq.html*>

Maintain a Vulnerability Management Program

5. Use and regularly update anti-virus software

Many vulnerabilities and malicious viruses enter the network via employees' email activities. Anti-virus software must be used on all email systems and desktops to protect systems from malicious software[7]

In accordance with the Visa USA PCI Data Security Standard, MICROS strongly recommends regular use and regular updates of anti-virus software. MICROS regularly tests new releases of anti-virus software releases from Norton® and McAfee® as well as security updates from Microsoft®, and provides weekly reports of test results to our distribution channel. Most updates are validated within 1 week, with critical updates validated sooner.

To make sure your anti-virus software is set up in compliance with Step 5 of the PCI Data Security Standard, "Use and regularly update anti-virus software", please consult Visa USA's website, "Cardholder Information Security Policy", <*http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html*>.

7. "PCI Security Audit Procedures", p. 20, V. 1.0, December 15, 2004. <*http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_tools_faq.html*>

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 via vendor security patches, and all systems should have current software patches to protect against exploitation by employees, external hackers, and viruses. For in-house developed applications, numerous vulnerabilities can be avoided by using standard system development processes and secure coding techniques[8]

MICROS uses separate development and production environments to ensure software integrity and security. Updated service packs and hot fixes are available via the MICROS product website, <http://www.micros.com>. While MICROS makes every possible effort to conform to Step 6 of the PCI Data Security Standard, certain parameters, including following change control procedures for system and software configuration changes, and the installation of available security fixes, depend on site-specific protocol and practices.

To make sure your site develops and maintains secure systems and applications in compliance with Step 6 of The PCI Data Security Standard, "Develop and Maintain Secure Systems and Applications", please consult Visa USA's website, "Cardholder Information Security Policy",*<http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html>*.

8. "PCI Security Audit Procedures", p. 21, V. 1.0, December 15, 2004. *<http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_tools_faq.html>*

Implement Strong Access Control Measures

7. Restrict access to data by business need-to-know

This ensures critical data can only be accessed in an authorized manner[9]

MICROS recognizes the importance of data control, and does so by establishing access based upon employee class level. This mechanism ensures access to sensitive information is restricted, password protected, and based on a need-to-know basis.

For more information on Step 7 of The PCI Data Security Standard, "Restrict access to data by business need-to-know", please consult Visa USA's website, "Cardholder Information Security Policy", <*http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html*>

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

This ensures that actions taken on critical data and systems are performed by, and can be traced to, known and authorized users[10]

MICROS recognizes the importance of establishing unique ID's for each person with computer access. No two MICROS users can have the same ID, and each person's activities can be traced, provided the client site maintains proper configuration and adheres to privilege-level restrictions predicated on a need-to-know basis. While MICROS makes every possible effort to conform to Step 8 of the PCI Data Security Standard, certain parameters, including proper user authentication, remote network access, and password management for nonconsumer users and administrators, for all system components, depend on site specific protocol and practices.

MICROS strongly recommends applying these guidelines not only to MICROS users, but to Windows users as well.

RES 3.2 SP 7 HF 5 allows merchants to require unique password logic for access to all Back of House/administrative functions.

MICROS recommends that all passwords be rotated on a regular basis not greater than 90 days.

9. "PCI Security Audit Procedures", p. 26, V. 1.0, December 15, 2004. <*http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_tools_faq.html*>
10. "PCI Security Audit Procedures", p. 27, V. 1.0, December 15, 2004. <*http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_tools_faq.html*>

For more information on Step 8 of the PCI Data Security Standard, "Assign a unique ID to each person with computer access", please consult Visa USA's website, "Cardholder Information Security Policy", <*http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html*>.

9. Restrict physical access to cardholder data

Any physical access to data or systems that house cardholder data allows the opportunity to access devices or data, and remove systems or hardcopies, and should be appropriately restricted[11]

In accordance with the Visa USA PCI Data Security Standard, MICROS strongly recommends restricting physical access to cardholder data. This includes physical access to the store server and any computer consoles capable of accessing the store server, as well as restricting physical access to customer credit cards during the payment process. MICROS recommends that restaurants secure their server in a locked office with limited access and suggest the use of handheld terminals by wait staff for credit card payment, so that payment can be accomplished tableside and the credit card never leaves the customer's sight.

To make sure your site is set up in compliance with Step 9 of The PCI Data Security Standard, "Restrict physical access to cardholder data", please consult Visa USA's website, "Cardholder Information Security Policy", <*http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html*>.

11. "PCI Security Audit Procedures.doc", p. 33, V. 1.0, December 15, 2004. <*http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_tools_faq.html*>

Regularly Monitor and Test Networks

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[12]

RES 3.2 SP 7 HF5 includes an audit log (MICROS Security Log) of all programming activity related to credit card data security, all access to credit card data, and all POS administrative activity. MICROS recommends that this log be enabled and archived for at least 1 year. The MICROS Security Log is enabled by default and cannot be disabled. To view/manage this log, open the Microsoft Event Viewer (*Windows* Start | Control Panel | Administrative Tools) and select the MICROS Security Log.

To make sure your site is in compliance with Step 10 of The PCI Data Security Standard, "Track and monitor all access to network resources and cardholder data", please consult Visa USA's website, "Cardholder Information Security Policy", <*http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html*>.

12. "PCI Security Audit Procedures", p. 37, V. 1.0, December 15, 2004. <*http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_tools_faq.html*>

11. Regularly test security systems and processes

Vulnerabilities are continually being discovered by hackers/researchers and introduced by new software. Systems, processes, and custom software should be tested frequently to ensure security is being maintained over time and through changes[13]

In accordance with the Visa USA PCI Data Security Standard, MICROS strongly recommends regular testing of security systems and processes. To make sure your site's security systems and processes are setup in compliance with Step 11 of The PCI Data Security Standard, "Regularly test security systems and processes", please consult Visa USA's Web site, "Cardholder Information Security Policy", *<http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html>*.

Maintain an Information Security Policy

12. Maintain a policy that addresses information security

A strong security policy sets the security tone for the whole company, and lets employees know what is expected of them. All employees should be aware of the sensitivity of the data and their responsibilities for protecting it[14]

In accordance with the Visa USA PCI Data Security Standard, MICROS strongly recommends maintaining a policy that addresses information security. To make sure your information security policy is setup in compliance with Step 12 of The PCI Data Security Standard, "Maintain a policy that addresses information security", please consult Visa USA's Web site, "Cardholder Information Security Policy",*<http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html>*.

13. "PCI Security Audit Procedures", p. 41, V. 1.0, December 15, 2004. *<http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_tools_faq.html>*

14. "PCI Security Audit Procedures.doc", p. 44, V. 1.0, December 15, 2004. *<http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_tools_faq.html>*

Credit Card Security Installation Checklist

This checklist should be reviewed with the customer and maintained by the installing entity as evidence that proper credit card security procedures were reviewed with the customer.

Version of RES Software Installed_____

Credit Card Driver Installed_____

Version of Credit Card Driver Installed_____

	Yes/No	Comments
Verify existence of a properly configured Firewall.		
Verify Tender/Media options are selected to mask the Credit Card Number and Expiration Date for all credit cards.		
Verify that the operating system's Login Passwords are changed from the default.		
Verify that the vendor-supplied passwords are changed from the default.		
Verify access points use complex passwords and that those passwords have been changed from vendor default.		
Verify that password settings are in compliance with PCI requirements for RES V3.2 SP7 HF5 and that each person has a unique user ID.		
Verify anti-virus software is installed and up-to-date. Verify that a plan is in place to keep anti-virus software updated.		
Verify that the RES Server is in a secure location with restricted physical access.		
Verify the MICROS Security Log is recording changes.		
Validate that the log is being properly archived.		

Micros Agent or Representative

Name_____

Company_____

Date_____

Signature_____

Merchant

Name_____

Company_____

Date_____

Signature_____