RES Version 3.2 Service Pack 7 Hotfix 6 with Transaction Vault Electronic Payment Driver Version 4.3 or Higher Payment Application Best Practices Implementation Guide

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 6 with Transaction Vault Electronic Payment Driver Version 4.3 or higher installed for electronic payment processing.

Declarations

Warranties

Although the best efforts are made to ensure that the information in this document is complete and correct, MICROS Systems, Inc. makes no warranty of any kind with regard to this material, including but not limited to the implied warranties of marketability and fitness for a particular purpose.

Information in this document is subject to change without notice.

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information recording and retrieval systems, for any purpose other than for personal use, without the express written permission of MICROS Systems, Inc.

MICROS Systems, Inc. shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this document.

Trademarks

FrameMaker is a registered trademark of Adobe Corporation.

Microsoft, Microsoft Excel, Win32, Windows, Windows®95, Windows 2000 (Win2K), and Windows NT are either registered trademarks or trademarks of Microsoft Corporation in the U.S. and/or other countries.

Visio is a registered trademark of Visio Corporation.

All other trademarks are the property of their respective owners.

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].

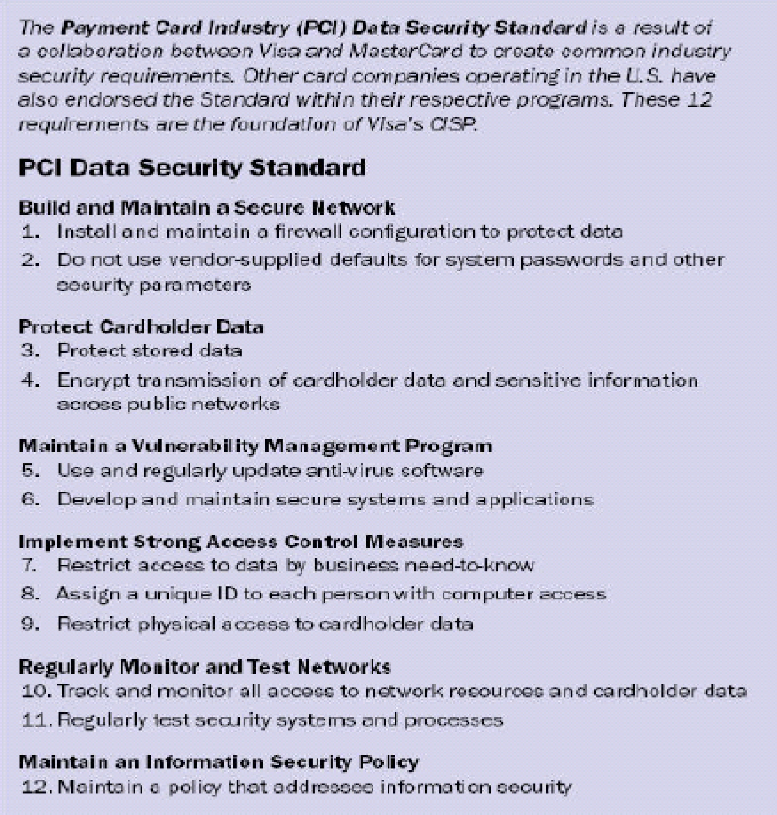
For more detailed information concerning PCI compliance, please refer to the Visa USA CISP website, <*http://usa.visa.com/download/business/accepting_visa/ops_risk_management/cisp.html*>.

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 commerce. 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 PCI requirements. Other card companies operating in the U.S. have also endorsed the PCI Data Security Standard within their respective programs.

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

Using the PCI Data Security Standard as its framework, PCI 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 "PCI_overview.pdf", <*http://usa.visa.com/download/business/accepting_visa/support_center/cisp_overview.pdf?it=c|/business/accepting_visa/ops_risk_management/pci%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 6 with Transaction Vault Version 4.3 or Higher 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 PCI 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 6 with Transaction Vault Version 4.3 or higher 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/merchants/risk_management/cisp.html*>

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 Systems, Inc. strongly 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", V. 1.1, September, 2006. <*https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf*>

Personal firewall software must be installed on any employee-owned computers with direct connectivity to the Internet, such as laptops used by employees, which are used to access the organization’s network. The firewall software’s configuration settings must not be alterable by employees.

Because of the Visa USA PCI Data Security Standard, MICROS Systems Inc. mandates that each site ensure that PCs, databases, wireless access points, and any medium containing sensitive data reside behind a firewall. The firewall configuration must restrict connections between publicly accessible PCs and any system component storing cardholder data, including any connections from wireless networks.

MICROS does not recommend a specific vendor’s firewall be installed. Work with the customers’ network administrator to setup something that works with their configuration. MICROS does sell a firewall that can be used for MICROS RES sites. For information on the hardware firewall that MICROS offers refer to *PMA05-828.*

Windows XP Pro, 2003, and Vista have a built in software firewall that should be enabled when running MICROS RES. The firewall should be enabled before installing the MICROS RES software.

To make sure your firewall configuration is set up in compliance with Requirement 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 6 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.

[4] “PCI Security Audit Procedures”, V. 1.1, September, 2006. <*https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf*>

List of Database Users

DBA

MICROS

CAEDC

DBSRPC

EOSAPPS

ESD

GSSCFG

GSSSERVER

KDSSERVER

REPORTS

REPORTUSER

SETUP

SYSCFG

PROCEDURES

EMPREPL

INSTALLER

MANAGER

RES 3.2 SP 7 HF 6 with Transaction Vault requires a Windows user to be active on the system. After the software has been installed, be sure to change the user’s password to something complex.

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.

Strong application and system passwords must be used whenever possible. MICROS Systems, Inc. mandates that customers and resellers/integrators must always create PCI compliant complex passwords.

For wireless environments, change wireless vendor defaults, including but not limited to, wireless equivalent privacy (WEP) keys, default service set identifier (SSID), password, and SNMP community strings. Disable SSID broadcasts. Enable Wi-Fi protected access (WPA and EPA2) technology for encryption and authentication. For more information, refer to the *MICROS Wireless Networking Best Practices: A Payment Application Best Practices (PABP) Implementation Guide Supplement* document.

All non-console administrative access must be encrypted using technologies such as SSH, VPN, or SSL/RLS (transport layer security) for web-based management and other non-console administrative access. Telnet or rlogin must never be used for administration.

For more information on Requirement 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 SP 7 HF 6 with Transaction Vault store sensitive track data.

[5] “PCI Security Audit Procedures”, V. 1.1, September, 2006. <*https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf*>

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 6 with Transaction Vault, the existing masking option bits have been enhanced to provide masking 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.

All credit authorization data stored within the system is purged on a regular basis. When a site upgrades from an earlier version of MICROS RES (Version 3.2 SP 7 HF 4 or lower) the database conversion process manages securing historical data.

Historical data stored on the system must be securely removed as a necessary component of PCI compliancy. Therefore, upgrades from a non-PCI compliant version to a PCI compliant version must include securely erasing all old databases, log files, and any other files containing sensitive data. For more information refer to the *MICROS RES Credit Card Security Guidelines, MD0003-124* document.

In some situations, MICROS RES resellers/integrators might be tasked with troubleshooting an issue with the system. To ensure cardholder data is protected, MICROS Systems, Inc. mandates MICROS RES resellers/integrators must only collect customer data (for example, sensitive authentication data, log files, debug files, databases, etc.) needed to solve a specific problem. Such data must only be stored in specific, known locations with limited access. Resellers/ integrators must only collect the limited amount of data needed to solve a specific problem and must encrypt such sensitive authentication data while stored. After such data is no longer used, it must be immediately deleted in a secure manner.

When troubleshooting customer issues, resellers and integrators must keep in mind the following when using databases from live customer sites:

- Collect live customer databases only when needed to solve a specific problem. If customer support requires the database, then it should be transferred to the MICROS customer support FTP site. Please refer to the *MICROS FTP Site File Transfer Policy.*
- Store databases in specific, known locations with limited access. Password protect zip archives used to store customer databases.
- Collect only the limited amount of data needed to solve a specific problem. Pull the latest known database backup, not every backup in the *\DbBackups* directory. The more files you retrieve, the more you have to manage through the troubleshooting process, and the more files you will have to destroy later. For information on destroying these files refer to the *MICROS Secure Wipe Tool* documentation.
- Securely delete such data immediately after use. This involves removing data from the PC or terminal where the troubleshooting occurred.

For more information, refer to the *Customer Support Information Security Guidelines* document located in the Member Services section of the MICROS website (*www.members.micros.com*).

For more information on Requirement 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 SP 7 HF 6 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).

Wireless transmissions of cardholder data must be encrypted over both public and private networks. Encrypt transmissions by using Wi-Fi Protected Access (WPA or WPA2) technology, IPSEC VPN, or SSL/TLS. Never rely exclusively on wired equivalent privacy (WEP) to protect confidentiality and access to a wireless LAN. Use one of the above methodologies in conjunction with WEP at 128 bit, and rotate shared WEP keys quarterly and whenever there are changes in personnel who have access to keys. WEP must be used with a minimum 104-bit encryption key and 24 bit-initialization value. Always restrict access based on media access code (MAC) address.

Because of the Visa USA PCI Data Security Standard, MICROS Systems Inc. mandates each site use some sort of encryption (VPN, SSL, etc) when sending any sensitive information over the Internet, including wireless connections, E-mail, and when using services such as Telnet, FTP, etc.

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 Requirement 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”, V. 1.1, September, 2006. <*https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf*>

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 Requirement 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*>.

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 Requirement 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 Requirement 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*>.

[7] "PCI Security Audit Procedures", V. 1.1, September, 2006. <*https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf*>

[8] "PCI Security Audit Procedures", V. 1.1, September, 2006. <*https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf*>

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. Access to customer passwords by reseller/integration personnel must be restricted.

For more information on Requirement 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 RES 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 Requirement 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 6 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”, V. 1.1, September, 2006. *<https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf>*

[10] “PCI Security Audit Procedures”, V. 1.1, September, 2006. *<https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf>*

Furthermore, MICROS Systems, Inc. advises users to control access, via unique usernames and PCI-compliant complex passwords, to any PCs, servers, and databases with payment applications and cardholder data.

MICROS Systems, Inc. mandates a two-factor authentication for remote access to the site's network by MICROS Systems, Inc. employees, administrators, and third parties. Technologies such as remote authentication and dial-in service (RADIUS), terminal access controller access control system (TACACS) with tokens, or VPS based on SSL/TLS or IPSEC with individual certificates must be used.

Remote Access

Remote access software security features must always be used and implemented. Therefore, default settings in the remote access software must be changed so that a unique username and complex password is used for each customer. Never use the default password and adhere to the PCI DSS password requirements established in Requirement 8 on page 14. The new password must contain a minimum of 8 characters, including a combination of numbers and letters.

Connections must only be allowed from specific, known IP/MAC addresses. Strong authentication or complex passwords for logins must be used. Encrypted data transmission and account lockout after a certain number of failed attempts must be enabled. The systems must be configured so that a remote user must establish a Virtual Private Network (VPN) connection via a firewall before access is allowed. Logging functions must be enabled for security purposes. Access to customer passwords must always be restricted. For more information, refer to the *Visa PCAnywhere Instructions* document and the *Webex Policy* document.

For more information on Requirement 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 table side and the credit card never leaves the customer's sight.

To make sure your site is set up in compliance with Requirement 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/merchants/risk_management/cisp.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 HF 6 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. Live sites should ensure that sales journals are enabled for each workstation. This file will track all transactions that occur on the workstation.

[11] "PCI Security Audit Procedures", V. 1.1, September, 2006. <*https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf*>

[12] "PCI Security Audit Procedures", V. 1.1, September, 2006. <*https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf*>

For troubleshooting and investigative purposes, each workstation writes to a debug log file. The debug log is always enabled, and requires no merchant, reseller, or integration interaction. This log file is located at the following path unless otherwise specified by the user:

\Micros\RES\POS\Etc

To make sure your site is in compliance with Requirement 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*>.

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 Requirement 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/merchants/risk_management/cisp.html*>.

[13] “PCI Security Audit Procedures”, V. 1.1, September, 2006. <*https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf*>

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. A site's maintained information security policy should include information on physical security, data storage, data transmission, and system administration. To make sure your information security policy is setup in compliance with Requirement 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>*.

[14] "PCI Security Audit Procedures", V. 1.1, September, 2006. *<https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf>*

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 SP 7 HF 6 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_____________________________________