RES Version 4.3 Hotfix 1 or Higher Payment Application-Data Security Standard (PA-DSS) Implementation Guide

General Information

About This Document

This document is intended as a quick reference guide to provide guidance and instructions for customers, resellers, and integrators to implement RES software into a merchant environment in a PCI DSS compliant manner. This document relates specifically to the MICROS Restaurant Enterprise Solution (RES) Versions listed below.

- RES 4.3 Hotfix 1 and higher

Taking the appropriate steps to secure your system is required in order to be PCI compliant.

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.

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 PCI 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 the PCI Data Security Standard was instituted. The program is intended to protect 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 PCI Security Standards Council website, https://www.pcisecuritystandards.org/.

About The PCI Data Security Standard

PCI compliance is required of all merchants and service providers that store, process, or transmit cardholder data. The program applies to all payment channels, including retail (brick-and-mortar), mail/telephone order, and e-commerce. To achieve compliance with PCI, merchants and service providers must adhere to the 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 among the credit card industry and is designed to create common industry security requirements, incorporating the PCI requirements.

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, listed below, consists of twelve basic requirements supported by more detailed sub-requirements:

The PCI Data Security Standard[2]

Build and Maintain a Secure Network

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

1. Reprinted from "Cardholder Information Security Program", <http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html>.
2. Reprinted from the 'PCI DSS Requirements and Security Assessment Procedures, v1.2' document, available on the PCI Security Standards Council website, https://www.pcisecuritystandards.org/.

Protect Cardholder Data

- **Requirement 3:** Protect cardholder data
- **Requirement 4:** Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

- **Requirement 5:** Use and regularly update ant-virus software
- **Requirement 6:** Develop and maintain secure systems and applications

Implement Strong Access Control Measures

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

Regularly Monitor and Test Networks

- **Requirement 10:** Track and monitor all access to network resources and cardholder data
- **Requirement 11:** Regularly test security systems and processes

Maintain an Information Security Policy

- **Requirement 12:** Maintain a policy that addresses information security

PCI Compliance and Windows NT

Although the Windows NT platform is supported by the RES product, this platform is not PA-DSS compliant and cannot be used in a PA-DSS compliant site.

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 Windows 2000, Microsoft Windows XP Pro, or Windows 2003
- Familiarity with the MICROS RES software
- Familiarity with operating MICROS peripheral devices

RES and the PCI Data Security Standard

PCI Data Security Standard

While MICROS Systems Inc. recognizes the importance of upholding cardmember 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. Information within this section pertains only to how the RES Version 1.0 software conforms to The PCI Data Security Standard.

To ensure the payment application is implemented into a secure network environment, RES does not interfere with the use of network address translation (NAT), port address translation (PAT), traffic filtering network device, anti-virus protection, patch or update installation, or use of encryption.

For a complete description of the PCI Data Security Standard, please consult the PCI Security Standards Council website https://www.pcisecuritystandards.org/.

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 software.

Build and Maintain a Secure Network

1. Install and maintain a firewall configuration to protect cardholder 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 PCI Data Security Standard, MICROS Systems Inc. mandates every site, including wireless environments, 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. "Payment Card Industry (PCI) Data Security Standard.doc", p. 4, V. 1.1, September, 2006. <https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf>.

Personal firewall software must be installed on any mobile and 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 PCI Data Security Standard, MICROS Systems Inc. mandates each site ensure that servers, databases, wireless access points, and any medium containing sensitive data reside behind a firewall. The firewall configuration must restrict connections between publicly accessible servers and any system component storing cardholder data, including any connections from wireless networks.

The firewall configuration must also place the database in an internal network zone, segregated from the demilitarized zone (DMZ) with the web server. A DMZ can be used to separate the Internet from systems storing cardholder data.

MICROS Systems, Inc. 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 Systems, Inc. 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 ensure 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 the PCI Security Standards Council website https://www.pcisecuritystandards.org/.

2. Do not use vendor-supplied defaults for system passwords and other security parameters

Hackers (external and internal to a company) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known in hacker communities and easily determined via public information.[4]

RES allows for all application, operating system, and database passwords to be changed.

4. "Payment Card Industry (PCI) Data Security Standard.doc", p. 5, V. 1.1, September, 2006. <https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf>.

Passwords that are complex should be on by default for all administrators and employees who have access to administrative functions.

MICROS is not permitted to manage these passwords for you. *Appendix A* of this document provides a sample log sheet for all password management. This section can be found beginning on page 27.

Default settings MUST be changed before a site goes live in order to maintain PCI compliancy. At a minimum, all passwords should be changed every 90 days.

MICROS Systems, Inc. advises against using any administrative accounts, such as the “sa” account for application access to the database, for application logins. Customers and resellers/integrators are advised to always assign strong passwords to these default accounts even if these accounts are not used. These default accounts should then be disabled or not used.

When a request for support is made to your support organization or to a third party vendor, they may need one or more of these passwords to do their job. Any time that a password is given out, it should be changed to maintain PCI compliancy.

Additionally, RES has the capability to enforce complex passwords for access to all Back Office applications, including programming, reporting, and Back Office utilities. Complex passwords can be enforced, including minimum length, alphanumeric passwords, periodic rotation, and lockout after failed log-in attempts. MICROS recommends that customers using RES implement complex passwords for access to Back Office applications in accordance with PA-DSS.

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.

Customers and resellers/integrators are advised to control access, via unique username and PCI DSS-compliant complex passwords, to any PCs, servers, and databases with payment applications and cardholder data.

Implementing RES Complex Security

Strong application and system passwords must be used whenever possible. MICROS Systems, Inc. mandates customers and resellers/integrators to always create PCI DSS-compliant complex password to access the payment application.

Follow these steps to implement RES Complex security:

1. Open the *POS Configurator* | *System* | *Restaurant* | *Security* tab, and disable the **Use Classic Security** option.
2. Configure the complex security settings according to the merchant's rules. The merchant must adhere to PCI guidelines in order to maintain PCI compliancy.

   The table below lists the available options, and the minimum recommended settings. All options are located on the *POS Configurator* | *System* | *Restaurant* | *Security* tab.

Option	Recommended Setting
Use Micros Classic Security	Always disabled.
Days Until Password Expires	90 Days
Minimum Password Length	7 characters. Password should contain both numeric and alphabetic characters.
Maximum Idle Time in Minutes	15 minutes
Maximum Failed Logins	6 attempts
Require AlphaNumeric Passwords	Always set to Enabled
Password Repeat Interval	4

RES Database User

There are two database users required to run RES; the DBA user, and the Micros user. The passwords for these two database users must be changed upon going live and further maintained by changing them every 90 days in order to maintain PCI compliancy.

Third Party Application Support

The RES system permits integration with third party vendors. The merchant is responsible for managing this integration with the RES system. If the vendor needs database access, or RES application access, the merchant is responsible for setting this up and for maintaining it. If utilizing third party support, MICROS recommends the following:

- Separate database user accounts should be set up for each vendor and their data access limited to what they need.
- Separate RES application user accounts should be set up for each vendor and their data access limited to what they need.
- RES Database DBA or MICROS passwords should not be given out. If they are given for support reasons, they should be changed immediately after use.

Wireless Environments

For wireless environments, change wireless vendor defaults, including but not limited to, wireless equivalent privacy (WEP) keys, default service set identifier (SSID), default passwords, and SNMP community strings. Disable SSID broadcasts and enable Wi-Fi protected access (WPA2) technology for encryption and authentication. **This must be done to maintain PCI compliancy.** For more information, refer to the *MICROS Wireless Networking Best Practices: A Payment Application Data Security Standard (PA-DSS) 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 the PCI Security Standards Council website https://www.pcisecuritystandards.org/.

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 an authorization.**

   Under no circumstances will RES store complete 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, the existing masking option bits are still in place. For credit card number (PAN) the system masks all but the last four digits. The expiration date is masked completely and the Cardholder name is not printed. Masking occurs from any printout or display device where it might be viewed by an unauthorized person. This includes workstation displays, peripheral devices (pole displays, hand-helds, PIN pads), as well as system reports, journals and log entries.

   The following options MUST be set before the site goes live, in order to maintain PCI compliancy:

   - **POS Configurator | Sales | Tender/Media | CC Tender | Mask Credit Card Number.** Option must be enabled.
   - **POS Configurator | Sales | Tender/Media | CC Tender | Mask Expiration Date.** Option must be enabled.
   - **POS Configurator | Sales | Tender/Media | CC Tender | Mask Cardholder Name.** Option must be enabled. When this option is enabled, the cardholder name is not saved to the database.

All credit authorization data stored within the RES system is encrypted, and is purged on a regular basis. Purging of credit card information should be set according to your processor's recommendations. Cardholder data exceeding the merchant-defined retention period must be purged.

5. "Payment Card Industry (PCI) Data Security Standard.doc", p. 6, V. 1.1, September, 2006. <https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf>.

To configure credit card purging go to the *POS Configurator* | *System* | *Restaurant* | *Business Settings* tab and enter a value in the *Save Batch Records* | *Number of Days* field. This value should be **15 days**.

Securely Deleting Historical Data

Historical data (magnetic stripe data, card validation codes, PINs, or PIN blocks) stored by previous versions of MICROS software must be securely removed as a necessary component of PCI compliancy. Refer to the *RES Upgrade Best Practices* document for instructions on how to securely remove such data.

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 within the database.

Therefore, upgrades from a non-PCI compliant version to a PCI compliant version should include a format of all of the system's hard drives and an installation on all software. A second method would be to securely erase all old databases, log files, and any other files obtaining sensitive data.

Any cryptographic material, such as cryptographic keys used for computation or verification of cardholder data or sensitive authentication data stored by previous versions of the software, must also be securely removed as a necessary component of PCI compliancy. Refer to the *RES Upgrade Best Practices, MD0003-135* document for instructions on how to securely remove such data.

Collecting Sensitive Authentication Data for Troubleshooting

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 sensitive authentication 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.

***Note**: When using the CAPMS Driver with RES, the Devices | Interfaces | Log Transactions option bit should only be enabled for troubleshooting purposes. This option bit should always be disabled when not troubleshooting CAPMS transactions.*

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*).

Data Encryption

Sensitive credit card data (Personal account number, expiration date, customer name) is encrypted on the RES system when at rest. RES employs strong data encryption using industry-standard algorithms such as 3DES and AES.

RES stores information (data at rest) in three areas:

- the in-store database,
- the backup server database, and
- the SAR client (standalone resilience) database.

Each of these areas contains both sensitive and non-sensitive information. The server retains a copy of all three, but only the last two are kept locally on each client.

For the in-store database, RES 4.0 encrypts the entire database using standard AES encryption. This process is transparent to applications that are working within the RES system and are authorized to access the database via standard SQL tools. The encryption of the database file prevents unauthorized access through binary editors and/or hex dump utilities.

In addition to the primary database encryption, a second level of encryption is applied to sensitive data before it is stored in the database. This is done at the application level, by the program that writes the data to the database. When required, only those applications that need to will decrypt the data. For all other users, this data will appear encrypted when accessed via SQL tools.

The RES security paradigm requires the use of encryption keys in three areas:

- Encryption of the database.
- Encryption of the sensitive fields in the database.
- Encryption of sensitive data transmitted over the network.

RES allows the end user to change the passphrase for these two keys as often as desired. This will be referred to as key rotation. During key rotation of the database, the entire database must be unloaded and reloaded, and all historical information is re-encrypted. This may require up to several hours to complete, depending on the size of the database. During key rotation of the sensitive data the system will be down, and all the historical data will be re-encrypted with the new key.

These passphrases MUST be changed before the site goes live and then at least once a year thereafter to maintain PCI compliancy.

Use RES Database Manager to change your passphrases. The user is not required to enter their passphrase, RES Database Manager will automatically select a passphrase for you. This passphrase will be alpha-numeric.

RES also encrypts sensitive data transmitted between the POS client and the RES server. RES encryption is used for this transport encryption. The private and public key pair reside on the RES Server and the Backup Server. Each POS client only has the public key.

MICROS recommends the transport encryption key be changed at least once a year.

Use RES Database Manager to change your passphrases and transport encryption key.

Follow these steps to change the database, or the data passphrase key:

1. Open RES Database Manager
2. Go to the *Encryption key* tab.
3. Select the **Change Database** and/or **Change Data Key** option.
4. Press the **CHANGE ENCRYPTION KEY** button. The system will automatically select a new alpha-numeric passphrase for the site.

Follow these steps to change the Transport Key:

1. Open RES Database Manager.
2. Go to the *Encryption key* tab.
3. Select the **Change Transport Key** option.
4. Press the **CHANGE ENCRYPTION KEY** button.

For more information on Requirement 3 of The PCI Data Security Standard, "Protect stored data", please consult the PCI Security Standards Council website https://www.pcisecuritystandards.org/.

4. Encrypt transmission of cardholder data across open, 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 the a public network or the Internet *always* use SSL Version 3.0and when transmitting wirelessly, *always* use the highest level of encryption available. For more information, please refer to the *MICROS Wireless Networking Best Practices: A Payment Application Data Security Standard (PA-DSS) Implementation Guide Supplement* document.

Because of the PCI Data Security Standard, MICROS Systems Inc. mandates each site use secure encryption transmission technology (for example, IPSEC, VPN, or SSL/TLS) when sending cardholder information over public networks, including when using wireless connections, E-mail, and when using services such as Telnet, FTP, etc. When sending credit card numbers via email, customers and resellers must use an email encryption solution.

6. "Payment Card Industry (PCI) Data Security Standard.doc", p. 7, V. 1.1, September, 2006. <https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf>.

Modems should not reside in application servers unless absolutely necessary. If a modem is installed, it should be kept powered off or disabled except when needed. For added security, the modem should be configured to use automatic call back and data encryption. Firewalls will not protect against attacks via the modem.

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.

Sensitive data transmitted between the POS client and the server is encrypted with RSA (asymmetrical encryption mechanism) on wired and wireless networks. Additionally, RES 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 (or automatically if the technology permits) 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.

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, as well as application access passwords. The encryption key for sensitive data can be rotated by the end user.

The MICROS database file is encrypted via AES. The passphrase for the MICROS database can be changed by the 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 the PCI Security Standards Council website https://www.pcisecuritystandards.org/.

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 PCI Data Security Standard, MICROS Systems Inc. mandates 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 monthly reports of test results to our distribution channel. Most updates are validated within 1 week, with critical updates validated sooner.

Anti-virus software must be deployed on all systems commonly affected by viruses, particularly personal computers and servers.

To ensure 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 the PCI Security Standards Council website https://www.pcisecuritystandards.org/.

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 Systems Inc. uses standard system development processes to ensure software integrity and security, including maintaining separate development and production environments and ensuring the separation of duties between the development/test and production environments. Updated service packs and hot fixes are available via the MICROS product website, <http://www.micros.com>.

7. "Payment Card Industry (PCI) Data Security Standard.doc", p. 8, V. 1.1, September, 2006. <https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf>.
8. "Payment Card Industry (PCI) Data Security Standard.doc", p. 8, V. 1.1, September, 2006. <https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf>.

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 patches, depend on site specific protocol and practices.

In order to comply with Requirement 6 of the PCI standard, all Operating Systems (OS) must be patched and updated regularly. When a critical update is released, the site must install that update to ensure that system security is as strong as possible. Antivirus definitions must also be installed on all PCs, and should be kept up to date with the most recent virus definitions. Check the documentation provided by your antivirus software provider as well as for your Operating System for steps to ensure that your software is up to date.

Microsoft Windows XP Pro feature System Restore must be disabled and remain disabled to maintain PCI compliancy. To disable System Restore, follow the steps below:

1. From the *Start Menu* go to the *My Computer* | *Properties* | *System Properties* | *System Restore* tab and enable either the **Turn off System Restore** option or the **Turn off System Restore on all drives** option.
2. Select **[Ok]**.
3. When prompted with the following message, click **[Yes]** to confirm that you would like to turn off the System Restore:

   ```
   You have chosen to turn off System Restore. If you
   continue, all existing restore points will be deleted,
   and you will not be able to track or undo changes to
   your computer.
   Do you want to turn off System Restore?
   ```

4. The *System Properties* dialog box will close. Follow the steps to turn on System Restore.

Follow these steps to turn on System Restore:

1. From the *Start Menu* go to the *My Computer* | *Properties* | *System Properties* | *System Restore* tab.
2. Clear the **Turn off System Restore** option or the **Turn off System Restore on all drives** option.
3. Click **[Ok]**.
4. The *System Properties* dialog box will close.

To ensure 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 the PCI Security Standards Council website https://www.pcisecuritystandards.org/.

Implement Strong Access Control Measures

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

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

MICROS Systems Inc. recognizes the importance of data control, and does so by establishing access based upon employee job 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 resellers and 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 the PCI Security Standards Council website https://www.pcisecuritystandards.org/.

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 Systems Inc. recognizes the importance of establishing unique IDs 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 based on a need-to-know basis.

While MICROS Systems Inc. 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 non-consumer users and administrators, for all system components, depend on site specific protocol and practices.

9. “Payment Card Industry (PCI) Data Security Standard.doc”, p. 9, V. 1.1, September, 2006. <https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf>.
10. “Payment Card Industry (PCI) Data Security Standard.doc”, p. 10, V. 1.1, September, 2006. <https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf>.

All merchants MUST apply these guidelines to all users on the system in order to maintain PCI compliancy.

Creating Secure Passwords

To comply with Requirement 8 of the PCI Data Security Standard, RES allows customers to require complex password logic for access to all Back of House/ administrative functions. Complex password logic will require that a valid user name and password be entered for access to all applications. The user name must be unique.

The following options are provided in POS Configurator on the *System* | *Restaurant* | *Security* form for the addition of complex passwords:

- **Days Until Expiration**
  Enter the number of days that a password may remain active before it must be changed.
  Required Setting: not greater than 90

- **Minimum Password Length**
  Enter the minimum number of characters required for the password length.
  Required Setting: at least 7

- **Password Repeat Interval**
  Enter the number of different passwords that must be used before an old password can be repeated.
  Required Setting: at least 4

- **Require Alphanumeric Passwords**
  Select this option to require passwords to contain letters and numbers.
  Required Setting: checked (enabled)

- **Maximum Allowed Failed Logins**
  Enter the number of failed logins that may occur before locking the user out of his/her account.
  Required Setting: not greater than 6

- **Maximum Idle Time**
  Enter the number of minutes an administrative application will remain idle before the application will undo any unsaved changes and exit, requiring the user to login again.
  Required Setting: no more than 15 minutes

To ensure strict access control of the RES application always assign unique usernames and complex passwords to each account. MICROS Systems Inc. mandates applying these guidelines to not only MICROS passwords but to Windows® passwords as well.

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.

Remote Access

MICROS Systems, Inc. mandates 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 Virtual Private Network (VPN) based on SSL/TLS or IPSEC with individual certificates must be used.

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 21 when creating the new, strong password for the remote access software. Never use the default password and adhere to the same PCI DSS password requirements when creating customer passwords. Passwords must contain at least 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. Disabling logs should not be done and will result in non-compliance with PCI DSS. Access to customer passwords must always be restricted to authorized reseller/integrator personnel. For more information, refer to the MICROS Customer Support Remote Support Access 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 the PCI Security Standards Council website https://www.pcisecuritystandards.org/.

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 PCI Data Security Standard, MICROS Systems Inc. mandates the restriction of physical access to cardholder data. Inbound and outbound traffic to the cardholder data environment must be restricted.

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.

MICROS Systems, Inc. mandates users not store cardholder data on Internet-accessible systems. To ensure cardholder is not stored on Internet-accessible systems, the web server and data server must not be on the same server.

To ensure your site is set up in compliance with Requirement 9 of The PCI Data Security Standard, "Restrict physical access to cardholder data", please consult the PCI Security Standards Council website https://www.pcisecuritystandards.org/.

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 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.

11. "Payment Card Industry (PCI) Data Security Standard.doc", p. 11, 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

Live sites should ensure that journals are enabled for each workstation. This file tracks all POS transaction activity that occurs.

To ensure 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 the PCI Security Standards Council website https://www.pcisecuritystandards.org/.

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 PCI Data Security Standard, MICROS Systems Inc. mandates regular testing of security systems and processes.

To ensure 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 the PCI Security Standards Council website https://www.pcisecuritystandards.org/.

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 PCI Data Security Standard, MICROS Systems Inc. mandates a maintained policy that addresses information security.

12. "Payment Card Industry (PCI) Data Security Standard.doc", p. 12, V. 1.1, September, 2006. <https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf>.
13. "Payment Card Industry (PCI) Data Security Standard.doc", p. 13, V. 1.1, September, 2006. <https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf>.
14. "Payment Card Industry (PCI) Data Security Standard.doc", p. 14, V. 1.1, September, 2006. <https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf>.

A site's maintained information security policy should include information on physical security, data storage, data transmission, and system administration.

MICROS Software Update Policy

MICROS Systems, Inc. may occasionally provide RES software updates remotely. As such, each site must develop usage policies for critical employee-facing technologies (for example, remote-access technologies, wireless technologies, removable electronic media, laptops, personal data/digital assistants (PDAs), e-mail usage, and Internet usage) to define proper use of these technologies for all employees and contractors.

Ensure these usage policies require the following:

- Require explicit management approval to use the devices.
- Require that all device use is authenticated with username and password or other authentication item (for example, token).
- Require a list of all devices and personnel authorized to use the devices.
- Require labeling of devices with owner, contact information, and purpose.
- Require acceptable uses for the technology.
- Require acceptable network locations for the technology.
- Require a list of company-approved products.
- Require automatic disconnect of modem sessions after a specific period of inactivity.
- Require activation of modems used by vendors only when needed by vendors, with immediate deactivation after use.
- Prohibit the storage of cardholder data onto local hard drives, floppy disks, or other external media when accessing such data remotely via modem.
- Prohibit cut-and-paste and print functions during remote access.

MICROS Systems, Inc. recommends all customers and resellers/integrators use a personal firewall product if computer is connected via VPN or other high-speed connection, to secure these "always-on" connections, per PCI DSS standards as documented on page 6.

To ensure 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 the PCI Security Standards Council website https://www.pcisecuritystandards.org/.

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, Cardholder Name, 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 defaults.		
Verify that complex password settings are in compliance with PCI requirements 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 also.		

MICROS Agent or Representative

Name_____

Company_____

Date _____

Signature_____

Merchant

Name_____

Company_____

Date _____

Signature_____

Appendix A

MICROS is not permitted to manage these passwords for you. This appendix provides a sample log sheet for all password management.

Remote Access

Vendors may connect remotely to your server to support you. This connection should be protected by a complex password.

Method	Username	Password	Date Changed

Windows

Each individual in your organization should also be given their own Windows Login. A separate Windows login should be given to each vendor.

Username	Password	Date Changed

Employees with Access to RES Applications

Each individual in your organization that needs access should be given their own RES Login. A separate RES login should be given to each vendor.

Employee	Username	Password	Date Changed
MICROS Support			
Property Expert			
Manager			

Database Users

Your RES database requires two user accounts be present. These accounts DBA and MICROS will need their passwords changed every 90 days. Each individual in your organization that needs direct database access should be given their own database login and should only be given access to what they need. A separate database login should be given to each vendor.

Username	Password	Date Changed
DBA		
MICROS		

Database Encryption

Your data is encrypted in three different ways: database, data, transport. The database and data encryption require the user to provide a passphrase.

Support requirements - this passphrase is used only to generate a random key - it is not needed after it is changed.

Type of Encryption	Date Changed