Got PCI?

micros®

At MICROS Systems, Inc., we feel it is important to inform, guide and educate our customers on important matters that may impact their businesses. We have put together this document to bring you up to date on some of the information that is available to our customers on the Information Security section of our public website, as well as the Payment Card Industry Security Standards Council (PCI-SSC) website. We have also included some tips and frequently asked questions. For complete information about PCI and your requirements, visit the PCI-SSC web site at: www.pcisecuritystandards.org.

Important Websites

PCI-SSC visit:
www.pcisecuritystandards.org

MICROS Information Security visit:
www.micros.com/ServicesAndSupport/InformationSecurity

MICROS Security Advisories visit:
www.micros.com/ServicesAndSupport/InformationSecurity/SecurityAdvisories

To receive notifications of MICROS Security Enhancements visit:
http://www.micros.com/ServicesAndSupport/InformationSecurity/SecurityEnhancements/DistributionOfSecurityRelatedPatches/

Common Abbreviations

PCI-DSS - Payment Card Industry Data Security Standards

PCI-SSC - Payment Card Industry Security Standards Council

QSA – Qualified Security Assessor

PA-DSS – Payment Application Data Security Standard

Why me?

Merchants who process, store or transmit cardholder data as part of authorization or settlement are required to comply with the terms of the Payment Card Industry Data Security Standard (PCI-DSS). This is because of a contract the Merchants have executed with their Acquiring Bank. As part of this contract, Merchants who are compromised and found to be non-compliant with the PCI-DSS can be subjected to heavy fines, penalties and charge backs by the cardholder industry. There are over 200 individual PCI-DSS line items that a Merchant must contractually comply with to be fully PCI-DSS compliant. A complete list of your requirements can be found on the PCI -SSC website at:

www.pcisecuritystandards.org, MICROS encourages you to visit this website and become intimate with the requirements of the PCI- DSS. For information specific to MICROS applications, we encourage you to visit the Information Security section of our public website at:
www.micros.com/ServicesAndSupport/InformationSecurity

Information about MICROS Security Advisories can be found at:
www.micros.com/ServicesAndSupport/InformationSecurity/SecurityAdvisories.

Please visit this website regularly, as PCI is a continuous process.

New MICROS system Install or upgrade in your future?

You have purchased a new MICROS system or decided it's time to upgrade your MICROS System to take advantage of some new product features. What should you do to make sure your MICROS application is installed to meet your PCI-DSS requirements?

For every PA-DSS validated MICROS product, MICROS produces a Best Practices Implementation Guide which describes how to configure and deploy the MICROS product in a secure manner.

For your convenience, MICROS has posted each of these guides on the Information Security Section of our public website at the following link:
http://www.micros.com/ServicesAndSupport/InformationSecurity/BestPracticesImplementationGuides/

Prior to the installation of your new system or upgrade of your existing system, you should determine the new version and discuss the guide with your installer. We also recommend you have them follow the Guide and keep a copy of the signed checklist in the Guide for your records.

What should I do about user names, passwords and remote support?

We have put together some recommendations for passwords and the remote support of your system to get you started:

- ✓ Delete or disable any weak or generic legacy usernames or passwords – this should include any in use by applications, operating systems, databases or remote support tools.

- ✓ Always use strong passwords – they should contain at least 7 characters using at least 3 of the following character types: lower case letters, upper case letters, numbers and symbols.

- ✓ Passwords should be changed at least once every 90 days

- ✓ User names and passwords should not denote a user's access level: for example, Administrator, MICROS or Support.

- ✓ User access should be granted on a need-to- know basis.

- ✓ User access should be promptly terminated in the event a user no longer requires access.

- ✓ You should not leave your remote access tool activated when not in use.

For complete answers to your questions about passwords and the remote support of your system as it relates to PCI compliance, consult a qualified QSA. A list of qualified QSAs is available on the PCI-SSC website at the following address: https://www.pcisecuritystandards.org/qsa_asv/find_one.shtml.

Other Important Information….

MICROS has many of its products tested by an independent Security Assessor and officially validated by the PCI-SSC as PA-DSS compliant. These validated MICROS products are listed on both the MICROS web site and the PCI-SSC web site.

The PCI-DSS requires you to install any security enhancements on your payment processing systems within 30 days of vendor release to the public. To facilitate this security update requirement for our customers, MICROS offers a free service on the Information Security section of our public web site at the following address: http://www.micros.com/ServicesAndSupport/InformationSecurity/SecurityEnhancements/DistributionOf SecurityRelatedPatches/

PCI Compliance is a continuous process. You should regularly check the Information Security section of www.micros.com and www.pcisecuritystandards.org for updates.

micros®

7031 Columbia Gateway Dr.
Columbia, MD 21046-2289
www.micros.com
For Sales Inquiries:
866-287-4736