



micros[®] PCI Compliance FAQ

What is the PCI Security Standards Council?

A Limited Liability Corporation (LLC) chartered in Delaware, USA, the Payment Card Industry Security Standards Council was founded by American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc.. All five payment brands share equally in the council's governance, have equal input to the PCI Security Standards Council and share responsibility for carrying out the work of the organization. The PCI Security Standards Council is an open global forum, that is responsible for the development, management, education, and awareness of the PCI Security Standards, including: the Data Security Standard (DSS), Payment Application Data Security Standard (PA-DSS), and Pin Transaction Security (PTS) Requirements. All of the five founding members have agreed to incorporate the PCI DSS as the technical requirements of each of their data security compliance programs.

What is the PCI-DSS?

The Payment Card Industry Data Security Standard, or "PCI-DSS", is a set of comprehensive requirements for enhancing payment account data security. The PCI-DSS was developed by the founding payment brands of the PCI Security Standards Council to help facilitate the broad adoption of consistent data security measures on a global basis. The PCI-DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data.

Who does the PCI-DSS apply to?

The PCI-DSS applies to any entity who is processing, storing or transmitting cardholder data.

Is the PCI-DSS a state or federal law?

No, the PCI-DSS is essentially a set of information security standards created by the Payment Card Industry Security Standards Council that are directed at Merchants who process, store or transmit cardholder data.

If the PCI-DSS is not a state or federal law, then why does a Merchant need to comply?

In order to accept credit cards, Merchants must sign an agreement with their Acquiring Bank. The language in this agreement varies with each Acquiring Bank, but typically holds the Merchant responsible for complying with the PCI-DSS and liable for all costs, including fines and penalties, assessed if the Merchant is compromised and found not to be PCI-DSS compliant.

What are the Visa PABP and PCI PA-DSS standards?

Visa developed the Payment Applications Best Practices, "PABP", guidelines to assist software vendors in creating secure payment applications that help Merchants and agents mitigate compromises, prevent storage of sensitive cardholder data (i.e. full magnetic stripe data, CVV, CVV2 or PIN data) and support overall compliance with the PCI Data Security Standard (PCI-DSS). Effective October of 2008, the Payment Card Industry Security Standards Council has taken this over from Visa and re-named the standard the Payment Application Data Security Standard, or PCI PA-DSS.

What is MICROS' responsibility relating to credit card security?

As a Payment Application Vendor and not a Merchant, MICROS is responsible for developing its products that process, store, or transmit cardholder data as part of authorization or settlement in compliance with the PCI PA-DSS standards. MICROS has been developing its products in compliance with the Visa PABP standards since Visa introduced the PABP program. Now that this program has been transitioned to the PCI Security Standards Council, MICROS develops its products as per the PCI PA-DSS and has its products validated by the PCI-SSC as PA-DSS compliant.

Is MICROS required by law to develop its products according to the PCI PA-DSS standards?

No, these are not state or federal laws. However, one of the 200+ PCI-DSS requirements for Merchants is to use a PA-DSS compliant payment processing application. So, MICROS customers who wish to be PCI-DSS compliant should be using a PA-DSS compliant version of our Point-Of-Sale or Property Management System products.

How can MICROS customers determine if the MICROS product they are using or contemplating purchasing is PA-DSS validated?

Customers who wish to verify that the product is PA-DSS validated can visit the PCI-SSC web site at the following link:

https://www.pcisecuritystandards.org/security_standards/vpa/

MICROS also publishes a list of PA-DSS validated products on its public web site at the following link:

<http://www.micros.com/NR/rdonlyres/E4170024-05DD-48BA-8E5A-459C345DC40F/0/MICROSSystemsIncProductValidationandExpirationScheduleJuly212010.pdf>

Is MICROS responsible for deleting any default or generic user accounts or passwords on its customer systems?

No. MICROS is not responsible for the creation, management or deletion of any user accounts or passwords. This is strictly the responsibility of the merchants.

Are merchants required to use only strong user accounts and passwords as part of being PCI-DSS compliant?

Yes, merchants are required to use passwords that are at least seven characters in length and consist of at least 3 of the following 4 character types: (upper case letters, lower case letters, numbers, symbols). Merchants are also required to change their passwords at least once every 90 days, and to immediately disable or delete any access credentials for any users who leave the organization or change jobs and no longer require access to the payment processing application.

Is MICROS Systems, Inc. required to take steps to ensure that its customers are PCI-DSS compliant?

No, it is the sole responsibility of the Merchant to ensure that it is PCI-DSS compliant. However, MICROS has issued multiple written correspondences to its direct customers advising them of the importance of PCI-DSS compliance, and the use of a PCI-PA-DSS certified payment application. These are all posted on the Information Security section of the MICROS web site at the following link:

<http://www.micros.com/ServicesAndSupport/InformationSecurity/SecurityAdvisories/>

What should MICROS customers do to determine their level of PCI-DSS compliance and to mitigate any gaps in order to become PCI-DSS compliant?

For information on assessing their level of PCI-DSS compliance, customers can visit the PCI Security Standards Council web site at: www.pcisecuritystandards.org.

Can MICROS Systems, Inc. assist its customers with their efforts to assess their level of PCI-DSS compliance or mitigation?

MICROS is not a Qualified Security Assessor "QSA" and cannot offer these services. For a list of certified QSA's, customers can visit the PCI Security Standards Council web site at:

https://www.pcisecuritystandards.org/pdfs/pci_qsa_list.pdf.

MICROS highly recommends that its customers engage the services of a QSA to assess their level of PCI-DSS compliance and to take appropriate steps to become PCI-DSS compliant.

Does MICROS provide its customers with copies of the documentation proving that its products are PCI PA-DSS certified?

These documents contain certain sensitive information and MICROS does not share these outside of the company. Customers who wish to verify that their MICROS product is PA-DSS validated can do so by visiting the PCI-SSC web site at the URL shown above in section 9. The PCI-SSC web site only lists payment processing products that are validated as PA-DSS compliant.

Does installing a PA-DSS validated payment processing application satisfy all of the PCI-DSS requirements?

No, although this is a very important part of PCI-DSS compliance, installing a PA-DSS validated payment application is only one element of PCI-DSS compliance. The PCI-DSS contains more than 200 individual requirements, most of which have nothing to do with the MICROS POS or PMS product. For more information on the PCI-DSS requirements, please visit the PCI Security Standards Council web site at: www.pcisecuritystandards.org

Should I contact MICROS to find out if I am PCI-DSS compliant?

No. Only the PCI Security Standards Council or a certified QSA is qualified to make this determination. MICROS strongly recommends that its customers take steps to ensure that they are PCI-DSS compliant. A good starting point is to visit the PCI Security Standards Council web site at: www.pcisecuritystandards.org . A list of certified QSA's can also be obtained from the PCI Security Standards Council web site at: https://www.pcisecuritystandards.org/pdfs/pci_qsa_list.pdf.

What is a "CPP"?

A Common Point-Of-Purchase, or "CPP", is a designation assigned to a Merchant by a Payment Brand when a pattern of fraudulent use of credit cards has been detected after these cards were used legitimately at this Merchant location.

What usually happens to a Merchant who has been designated as a CPP?

The Payment Brand and/or Acquiring Bank will usually require a forensic investigation be conducted by a QSA to detect and mitigate the cause(s) of the compromise. If the Merchant is determined to be out of compliance with the PCI-DSS during this investigation, the Merchant will also usually incur fines, penalties, charge backs, etc. that are not insignificant.

What role does MICROS play when one of its customers has been designated a CPP?

The role that MICROS can play is limited to answering technical questions about its products for either the QSA or law enforcement, and reviewing the forensic report. MICROS is not a QSA and is not qualified to conduct a forensic investigation in the event of a compromise.

Is MICROS responsible to pay some or all of its customers fines, penalties charge backs, etc. in the event that the customer is compromised?

No, these fines, penalties, etc, are the result of the merchant failing to confirm to the terms of their contract with their Acquiring Bank and have nothing to do with MICROS.

Are the MICROS Data Centers PCI-DSS compliant?

Our domestic, European, and Latin America Data Centers have been certified PCI-DSS compliant. Our Asia/Pacific Data Center is currently undergoing evaluation for PCI-DSS compliance.

Is MICROS a PCI-DSS Certified Service Provider?

Yes, for a list of Certified Service Providers, you can visit the Visa web site at:

http://usa.visa.com/download/merchants/cisp_list_of_cisp_compliant_service_providers.pdf?it=c/merchants/risk_management/cisp_service_providers.html>List%20of%20CISP-Compliant%20Service%20Providers.

Does MICROS conduct background checks on its perspective employees and contractors who have access to sensitive cardholder data?

Yes, MICROS conducts reference checks, criminal background checks and other important checks such as SSN, and DMV checks. MICROS also requires these checks be performed by its contractors and dealers.

How does MICROS keep up with the changing security standards?

MICROS is a Participating Organization with the PCI Security Standards Council. As Participating Organization, MICROS receives routine news and updates from the PCI Security Standards Council. MICROS also sits on the PCI-SSC Board of Advisors.

Has MICROS established remote support policy and standards for customer support?

Yes, MICROS has published a Remote Support Policy document which describes our approved methods of secure remote access. These have been reviewed and approved by our QSA. To obtain this document, please visit the MICROS web site at:

http://www.micros.com/NR/rdonlyres/35B1DED6-6D56-48E6-98A2-D0C58C34AD2E/0/REMOTE_SUPPORT_POLICY_2009.pdf

Does MICROS provide its customers with helpful Information Security related advisories?

Yes, MICROS maintains a special Information Security section on its public web site at the following link:

<http://www.micros.com/ServicesAndSupport/InformationSecurity/>

How does MICROS notify its customers of any security updates available for its products?

MICROS posts these on the Information Security section of its public web site at the link below. MICROS customers can sign up to receive automated email alerts each time MICROS releases a security update for its products.

<http://www.micros.com/ServicesAndSupport/InformationSecurity/SecurityEnhancements/>

Does MICROS offer a Best Practice Implementation Guide for its products to advise its customers on the proper and secure way to install its POS and PMS products?

Yes, for each PA-DSS validated version of each MICROS product, we publish a Best Practices Implementation guide on the Information Security section of our web site at the link below:

<http://www.micros.com/ServicesAndSupport/InformationSecurity/BestPracticesImplementationGuides/>

Does MICROS have a corporate Information Security Policy?

Yes, our Enterprise Information Security Policy can be found on the Information Security section of our web site at the following link:

<http://www.micros.com/NR/rdonlyres/72E62768-5BD3-471BB190-60169E42B977/0/MICROSystemsIncInformationSecurityPolicyv60March2009.pdf>