



MICROS-Fidelio Customer Support

Remote Support Access Policy

Europe, Africa & Middle East

A description of the policies and procedures relating to remote access to customer systems by MICROS-Fidelio Customer Support personnel. This document also includes MICROS-Fidelio's recommended connection and security methods as well as details on how PCI DSS, PABP and Sarbanes-Oxley requirements affect how MICROS-Fidelio customers are supported.

Document Version 3.10 ©2010 MICROS-Fidelio GmbH

Foreword

This document is provided by MICROS-Fidelio GmbH as a reference guide only and in no way implies that the recommendations described within will prevent unauthorized access to customer networks or systems. MICROS-Fidelio accepts no responsibility for the security of customer networks, systems, or applications. Please refer to your individual support maintenance contract or contact your local account or support manager for further details.

Additionally, MICROS-Fidelio does not provide PCI DSS assessments or audits and cannot provide review of or approval for customer network security strategies or policies.

MICROS-Fidelio Support is restricted to only providing support via the communication technologies described in this document.

*Document prepared by: M.I.S. Department Europe, Africa and The Middle East
MICROS-Fidelio GmbH ©2010*

Table 1: Change History

DATE	DESCRIPTION
09.09	Base document from Micros Inc.
01.10	Initial draft of EAME version
02.10	Micros newest policy (02.10) inclusion
03.10	Micros newest policy (03.10) inclusion
08.10	Webex to Bomgar replacement

Table of Contents

OVERVIEW	3
INTENDED AUDIENCE	3
REFERENCE DOCUMENTATION	3
EXECUTIVE SUMMARY	4
1. MICROS-FIDELIO RECOMMENDATIONS FOR SECURE REMOTE SUPPORT ACCESS	4
2. MICROS-FIDELIO POLICIES REGARDING SECURE REMOTE SUPPORT ACCESS	4
INDUSTRY REQUIREMENTS	5
1. PAYMENT CARD INDUSTRY (PCI) DATA SECURITY STANDARD (DSS)	5
MICROS-FIDELIO RECOMMENDATIONS	6
1. BUILD AND MAINTAIN A SECURE NETWORK	6
<i>Firewalls</i>	<i>6</i>
<i>User Accounts and Passwords</i>	<i>6</i>
2. PROTECT CARDHOLDER DATA	7
<i>Database Handling</i>	<i>7</i>
<i>Transport Encryption</i>	<i>7</i>
3. IMPLEMENT STRONG ACCESS CONTROL MEASURES	7
<i>BOMGAR</i>	<i>8</i>
4. REGULARLY MONITOR AND TEST NETWORKS	8
<i>Track and Monitor All Access to Network Resources and Cardholder Data</i>	<i>8</i>
REMOTE ACCESS AND SUPPORT SOFTWARE	8
1. CUSTOMERS WITH INTERNET ACCESS:	8
<i>BOMGAR</i>	<i>9</i>
<i>PCAnywhere</i>	<i>9</i>
2. CUSTOMERS WITH TRADITIONAL DIAL-UP MODEM ACCESS:	9
EXISTING REMOTE SUPPORT CONNECTIONS	10
VERIFICATION OF MICROS CALLERS	10
NOT SUPPORTED OR APPROVED	11

Overview

In order to maintain compliance with specific industry requirements such as the Cardholder Information Security Program (CISP), Payment Card Industry Data Security Standard (PCI DSS) and Payment Application Data Security Standard (PA-DSS), MICROS-Fidelio has developed standard policies controlling what methods are used to deliver remote support to customers from the MICROS-Fidelio Customer Support Centers. This document describes the MICROS-Fidelio recommended connectivity and security methods and supported remote access applications. It also provides details on user account and password management.



Intended Audience

This document is intended for MICROS-Fidelio customers as well as MICROS-Fidelio Support, Implementation, Sales, and Account Management professionals, MICROS-Fidelio VARs and Service Partners and any other audience interested in the remote support policies and procedures used by the MICROS-Fidelio Support Centers.

Reference Documentation

- The Payment Card Industry Security Standards Council (PCI-SSC) web site is available at: <https://www.pcisecuritystandards.org/>
- The latest version of the Payment Card Industry Data Security Standard (PCI-DSS) is available at: https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml
- A listing of Qualified Security Assessors (QSA's) is available from the PCI-SSC web site at: https://www.pcisecuritystandards.org/pdfs/pci_qsa_list.pdf
- A copy of the Payment Card Industry (PCI) Self-Assessment Questionnaire from the PCI-SSC is available at: <https://www.pcisecuritystandards.org/saq/index.shtml>
- General information on PCI compliance validation and requirements are available from VISA's web site at http://usa.visa.com/merchants/risk_management/cisp_merchants.html
- MICROS Inc. related PCI information is available at <http://www.micros.com/ServicesAndSupport/InformationSecurity/>
- MICROS Inc. related customer support policy is available at <http://www.micros.com/ServicesAndSupport/CustomerSupport/>

Executive Summary

1. MICROS-Fidelio Recommendations for Secure Remote Support Access

- Customers should implement and maintain secure network infrastructure and policies such as firewalls, Network Address Translation (NAT), Access Control Lists (ACL's), individual user-account-based authentication, and routine password rotation.
- Customers are advised to implement secure methods for remote support access that complies with the terms of the PCI-DSS.
- Customers should implement methods for logging user access to their networks and system(s) consistent with Section 10 of the PCI-DSS.
- Remote access applications and user accounts/passwords configured for use by MICROS-Fidelio Support should be enabled only when needed for remote access and should be disabled or removed immediately afterward.
- In addition to standard access controls, user accounts configured for remote access should include only those access rights required for the service/support being provided and should be robustly audited.



2. MICROS-Fidelio Policies Regarding Secure Remote Support Access

- MICROS-Fidelio will only provide remote support via solutions that have been tested and approved by MICROS-Fidelio Customer Support in accordance with PCI-DSS guidelines. Solutions not approved and supported by MICROS-Fidelio Customer Support can be nominated for approval through your Account Manager or Account Representative. A testing and validation fee may be charged to complete the approval process. Additional costs may be included if non-standard or unsupported software is required.
- MICROS-Fidelio Customer Support will not store or manage user account information or passwords for customer systems or applications. It is recommended that customers use unique and strong user-based accounts and passwords for network and application access. MICROS-Fidelio Customer Support is unable to provide assistance for issues involving lost or forgotten passwords or user account information.
- MICROS-Fidelio Application Support does not provide network configuration, implementation, or systems consultation services.

Industry Requirements

The PCI Security Standards Council (PCI SSC) was formed in 2006 by Visa, MasterCard, American Express, Discover and JCB to develop industry standards relating to the handling and storage of credit card data and credit card customer information. These standards comprise the Payment Card Industry Data Security Standard (PCI DSS). The PCI DSS details specific requirements relating to network security and access control. The following is a summary of those requirements which impact how MICROS provides remote support to its customers. Complete details on PCI DSS requirements can be found at www.pcisecuritystandards.org and should be reviewed in detail by each customer with their individual PCI DSS Qualified Security Assessor (QSA). *MICROS-Fidelio does not provide PCI DSS assessments or audits and cannot provide approval for customer network security strategies or policies.*

1. Payment Card Industry (PCI) Data Security Standard (DSS)

PCI DSS requirements are applicable to any networks or systems where credit card Primary Account Numbers (PAN) are stored, processed, or transmitted. These requirements apply to all MICROS-Fidelio products with the optional Credit Card (CA/EDC) module installed and active and applies to all "system components". The Council defines System Components as "... any network component, server, or application that is included in or connected to the cardholder data environment." Please refer to the PCI DSS for more detail.

The DSS is comprised of 12 General Requirements grouped in 6 Sections.

SECTION	GENERAL REQUIREMENT
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords or other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder 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

MICROS-Fidelio Recommendations

The following recommendations are provide as a guideline that should be followed to help ensure MICROS-Fidelio support personnel are able to provide you with remote support assistance without compromising your Information Security Policy.

1. Build and Maintain a Secure Network

Firewalls

MICROS-Fidelio recommends that all customers implement and maintain network access control appliances and/or software to control access to and from customer networks and systems (firewalls). Firewalls should include the use of Network Address Translation (NAT), Packet Filtering, Access Control Lists (ACL) and/or Application-Layer firewalls.

User Accounts and Passwords

All user accounts and passwords created during the installation and configuration of your MICROS-Fidelio product(s) should be removed, disabled, or passwords changed to unique, complex values as per the terms of the PCI-DSS. MICROS-Fidelio will *not* maintain or store user account information, including passwords, for your system.

MICROS-Fidelio recommends that unique user accounts with strong passwords are used for all users including any user accounts assigned for use by the MICROS-Fidelio Support Center. User accounts provided to MICROS-Fidelio Support for remote support access should be disabled when not in use.

For security purposes, effective July 1, 2010, MICROS-Fidelio will no longer store sensitive customer information such as user access credentials, user account information, remote access information, and passwords on its network. All existing information of this nature will be securely deleted from current secure storage locations within the MICROS-Fidelio network. MICROS-Fidelio Support will not create or modify any user accounts or account passwords on your system nor does MICROS-Fidelio Support have dedicated user accounts or “back door” accounts available. If a customer is unable to provide a login and password for access (if needed) to the MICROS-Fidelio application, database, or Operating System, MICROS-Fidelio may not be able to provide remote support. Therefore, MICROS-Fidelio strongly recommends that its customers designate someone on their staff to actively manage their user accounts and passwords and to be able to provide access to MICROS-Fidelio in the event that remote support is needed.

2. Protect Cardholder Data

Database Handling

Cardholder data is stored in a highly encrypted format within your PA-DSS Validated MICROS-Fidelio product's database (sensitive Track Two data is not stored by MICROS PA-DSS Validated products). From time to time it may be necessary for MICROS-Fidelio Support to obtain a copy of your database for testing or troubleshooting purposes. In such cases, MICROS-Fidelio might need to transfer a copy of the database via secure connection to the MICROS-Fidelio Support Center. Once testing and/or troubleshooting has completed, the database and any data generated from the database (i.e. reports, data exports, etc.) will be destroyed.

MICROS-Fidelio Customer Support will not accept databases from customer via email or unsecure file transfer. Databases can be mailed to MICROS-Fidelio Customer Support only by utilizing a tracking-based shipping method that requires an accepting signature (i.e. registered Post, FedEx, UPS, DHL, etc.).



Transport Encryption

Connectivity methods provided by customers must be capable of providing at least 128 bit encryption at the transport layer (SSL or IPSEC).

3. Implement Strong Access Control Measures

MICROS-Fidelio recommends that each customer provide remote access to be used by MICROS-Fidelio Customer Support via PCI-DSS compliant methods. Allowing access to your network and/or systems using unsecure methods or methods not conforming to PCI-DSS standards can leave you open to breach and loss of sensitive data as well as fines and other costs.

Implementation and maintenance of networks, network configurations, and network security are the responsibility of the customer. MICROS-Fidelio Systems Department provides support and consulting for network planning or development services.

BOMGAR

MICROS currently utilizes **BOMGAR Secure Remote Support Software** product for all remote support tasks, including the MICROS-Fidelio Customer Support. BOMGAR is an on-demand, secure, web based, remote access application. A "Support Session" can only be started via a cooperative exchange between the customer and a MICROS-Fidelio Customer Support agent. Once a Support Session is started the customer must grant access to either the entire system or an individual application(s). Application level access must be provided to the Support Agent by the customer as well. The authentication for the support agent is linked to the MICROS corporate ActiveDirectory domain user database.

4. Regularly Monitor and Test Networks

Track and Monitor All Access to Network Resources and Cardholder Data

MICROS-Fidelio recommends that customers implement methods for logging user access to their system(s) consistent with Section 10 of the PCI-DSS. Logging should be enabled both within the MICROS-Fidelio application(s) and at the Operating System level to ensure that all user access can be audited. See the Payment Card Industry Data Security Standard (PCI-DSS) document or consult your PCI Consultant or Qualified Security Assessor (QSA) for more information.

Remote Access and Support Software

Our current remote support policy now requires that MICROS-Fidelio employees and contractors only connect to customer's systems using a MICROS-Fidelio approved remote access tool that requires the customer to tactically grant access each time remote support is needed. This ensures that no MICROS-Fidelio personnel are ever connected to any customer systems without their express knowledge and consent. This policy actually exceeds the Payment Card Industry Data Security Standard (PCI-DSS) requirements and provides MICROS-Fidelio customers with a much improved level of security. MICROS-Fidelio has listed two approved remote access tools below. These are the only MICROS-Fidelio approved remote access tools at this time. Any other remote access tools or applications must be reviewed and approved by MICROS-Fidelio in writing.

1. Customers with Internet Access:

Currently, the only MICROS-Fidelio approved remote support tools for customer locations that have secure internet access are the BOMGAR Secure Remote Support Software or PCAnywhere v12.5 and higher.

BOMGAR is an on-demand, secure, web based, remote access application. A "Support Session" can only be started via a cooperative exchange between the customer and a MICROS-Fidelio Customer Support agent. Once a Support Session is started the customer must grant access to either the entire system or an individual application(s). Application level access must be provided for the Support Agent by the customer as well. MICROS-Fidelio support and Implementation personnel are licensed to use the BOMGAR Secure Remote Support Software. **MICROS-Fidelio customers do not need to purchase Bomgar in order to receive remote support from MICROS-Fidelio using this tool.** All that is needed is secure internet access.

PCAnywhere should only be used if the PCAnywhere Host on the customer system has been configured in a secure manner consistent with the recommendations outlined in the Appendix A: "Secure Configuration of PCAnywhere". The secure configuration of PCAnywhere includes:

- a. Symmetric or Public Key encryption enabled
- b. Logging enabled
- c. Account Lockout enabled
- d. Prompt to Confirm Connection enabled
- e. Use of unique user account and password for each support session
- f. PCAnywhere Host must be disabled when not in use

Customers wishing to use PCAnywhere will need to purchase and deploy the PCAnywhere application. This can be acquired from MICROS-Fidelio if desired.

2. Customers with Traditional Dial-Up Modem Access:

Beginning July 1, 2010, MICROS-Fidelio will only provide remote support services for customers with traditional dial-up modem access using PCAnywhere v12.5 and higher. Those customers wishing to use dial-up modem access with PCAnywhere are asked to review their configuration of PCAnywhere, and to follow the recommendations outlined in our document "Secure Configuration of PCAnywhere".

PCAnywhere cannot be used to provide remote support to customers across direct unsecured internet connections. MICROS-Fidelio recommends that all customers implement and maintain network access control appliances and/or software to control access to and from customer networks and systems (firewalls). Firewalls should include the use of Network Address Translation (NAT), Packet Filtering, Access Control Lists (ACL) and/or Application-Layer firewalls.

Existing Remote Support Connections

MICROS-Fidelio has to provide the security level outlined in this document to all customers. With this background, existing remote access solutions have to be reviewed and adapted to be fully PCI-DSS compliant.

Customers with *existing* VPN and/or dialup connections may choose from one of the following options:

1. VPN Tunnel connection will be removed and MICROS-Fidelio support will use BOMGAR connections in the future.
2. The VPN Tunnel connection will be removed and a secure dialup PCAnywhere connection, as detailed in this document, will be used for future remote support.
3. If it is agreed to keep the VPN Tunnel connection, the customer must create and maintain user/password credential sets to allow access to the network.
4. A secured PCAnywhere connection will be installed for use via the existing VPN-Tunnel
5. Existing remote connection will be kept as it is, but customer will sign a waiver provided by Micros.

Verification of MICROS Callers

As most communication between MICROS-Fidelio Support and its customers is initiated by MICROS-Fidelio customers, it is typically unnecessary for our customers to verify that the person on the telephone is actually a MICROS-Fidelio representative. However, in cases where MICROS-Fidelio contacts you and requests remote access to your system for a reason that you were previously unaware of, MICROS-Fidelio highly recommends that you verify the legitimacy of the caller before granting access to your network. This can be done by requiring the MICROS-Fidelio representative to provide you with the Clarify support case number for the particular support case he/she is contacting you about. Then, you can contact the MICROS-Fidelio Customer Support Center to verify the support case and caller.

Also, all remote connections by MICROS-Fidelio personnel using the BOMGAR Secure Remote Support Software will be made using the following domain:
eamesupport.microsdc.com

Not Supported or Approved

1. WebEx Remote Access Solution (a.k.a. SMARTech)
2. Other Remote Support Solutions like TeamViewer or LogMeIn
3. Unsecured/unencrypted direct internet connection (not using a VPN Tunnel) via PCAnywhere versions older 12.5, VNC, Microsoft Remote Desktop, DameWare or other remote access tools
4. Any remote access method that does not require the customer to grant access at the time the connection is being made to a system or network (e.g. static IPsec-tunnels).
5. Any remote access method which requires the installation of client software