



IMPORTANT SECURITY NOTICE

June 22, 2011

Dear Valued Customer:

While MICROS strongly recommends that our customers comply with all of the requirements of the Payment Card Industry Data Security Standard, (PCI-DSS), we feel that it is especially important to address four particular vulnerabilities:

Insecure Remote Access: Remote access tools, such as PCAnywhere, should not be left always-on and in active listening mode when not in use for legitimate business purposes. This provides the attackers with a method of easy ingress into your network. You should ensure that your remote access application is disabled at all times except when needed for a specific task. Please refer to the MICROS Information Security web site for more details:
<http://www.micros.com/ServicesAndSupport/InformationSecurity/>

No Firewall or Improperly Configured Firewall: If your network is connected to the internet, a properly configured firewall is absolutely critical. All non-essential incoming and outgoing traffic should be blocked to prevent unauthorized access via the internet. Please refer to the PCI-SSC web site for more details:
https://www.pcisecuritystandards.org/security_standards/

Anti-Virus/Anti-Malware Application: Although in many cases, a commercial anti-virus application may be deployed with a new system, many customers fail to renew the annual updates subscription. To be effective, it is imperative that an anti-virus application be deployed in active scanning mode and be maintained with the latest security updates at all times.

Generic User Accounts and Weak Passwords: The use of shared, generic or default user accounts, such as “service, administrator, manager”, etc. should be immediately discontinued. Each person accessing your network should have his/her own unique user name which should not denote their position or privilege level. Also, each user account should have a strong password (consisting of at least 7 characters and 3 different character types (i.e.) upper and lower case letters, numbers, symbols). User accounts should be promptly disabled or terminated if no longer needed or if inactive for 90 days. Passwords should be changed at least once every 90 days.

Please contact your MICROS representative if you have any questions.

Sincerely,

MICROS Systems, Inc.
Information Security