



Recommendations Regarding Remote System Access

Overview: Statistics show that a high percentage of system compromises occur due to poorly configured or maintained remote access applications. MICROS Systems, Inc. strongly recommends that you follow the guidelines outlined below to mitigate or prevent unwanted access or compromise.

Recommendations:

1. Each person with access to your system should have their own unique user name. You should never use default or generic user names, (i.e.) sales group, or eastern region. Also, your user names should not signify the access credentials of the user, (i.e.) administrator.
2. Each person with access to your system should use a strong password, which consists of at least 8 characters using at least three of the following character types: upper and lower case letters, numbers, symbols. Your password should not include your name or words found in the dictionary.
3. You should force all people with access to your system to change their password at least once every ninety days.
4. You should have a process in place that ensures that the access credentials for anyone leaving your organization, or transferring to another job that does not require the same level of access, be terminated or modified as soon as possible.
5. You should limit the level of access to your system, based on the user's need-to-know. Each user should have a legitimate business need to all information for which they have been granted access. For example, MICROS implementation or support should not have access to your entire network, but only the MICROS equipment that they must install, upgrade or support.
6. Users who access your system remotely should be required to use dual-factor authentication, or you should use a remote access tool that does not allow remote access to your system without your express approval.
7. If possible, you should shut down your remote access application when not in use and only enable this application when remote access to your system is required for service/support.
8. You should limit or restrict remote users from the internet whenever possible. This is to prevent the introduction of Viruses, Worms, Trojans, etc. to your system.
9. It is important for customers who process credit cards to comply with the Payment Card Industry Data Security Standard, (PCI-DSS). For more information about the PCI-DSS, please refer to the following link:
https://www.pcisecuritystandards.org/security_standards/pci_dss_download_agreement.html
10. Always protect your remote access credentials. Never leave passwords or user names where they are easily obtainable by an intruder, (such as in a file labeled "Passwords" on your PC).