SonomedEscalon™

CYBER SECURITY RECOMMENDATIONS

Master-Vu Ultrasound Systems

Master-Vu systems rely on user-provided PC computers that utilize Microsoft Windows version 7 or higher as their software Operating System. Failure to maintain cyber security could result in compromised device functionality, loss of data availability or integrity, or exposure of other connected devices or networks to security threats.

Sonomed Escalon recommends the following minimum procedures be followed in order to maintain a basic level of cyber security:

① **Utilize Device Only for Intended Use**. Limit or prohibit use of device for any purpose other than ophthalmic ultrasound, including Internet browsing and email, to limit potential exposure to cyber security risks.

② **Verify Windows Firewall is Enabled**
Device are shipped from the factory with the Windows Firewall on by default. Users should check periodically to make sure it hasn't been turned off.

IMPORTANT: If device is connected to a network, ensure that device is placed behind a strong network firewall.

③ **Install All Available Microsoft-Issued Updates for Windows Operating System**
Updates are made available at the Download Center of Microsoft's website.

④ **Install Windows-Compatible Anti-Virus Program**
The Operator should utilize an antivirus and antimalware program, and keep it current by regularly downloading updates from the program manufacturer's website. Many of these programs update automatically and can help protect the system from spyware and malicious software.

⑤ **Enable Windows 8 Bitlocker**
The Operator can use BitLocker Drive Encryption to help protect files on the entirety of the drive. BitLocker can help block hackers from accessing the system files they rely on to access sensitive data, or from accessing a disk drive by physically removing it from the system and installing it in a different one. New files are automatically encrypted when added to the disk drive that uses BitLocker. However, if these files are copied to another drive or a different PC, they're automatically decrypted. BitLocker can encrypt the drive Windows is installed on (the operating system drive) as well as fixed data drives (such as internal hard drives). The Operator can also use BitLocker To Go to help protect all files stored on a removable data drive (such as an external hard drive or USB flash drive).

For more information on cyber security, please consult your IT support staff and/or visit Microsoft Security www.microsoft.com/security.