Sonomed Escalon™

CYBER SECURITY RECOMMENDATIONS

VuMAX HD Ultrasound Systems

VuMAX HD systems incorporate Microsoft Windows 8 as their software Operating System and, as such, makes available to Operators the full scope of Microsoft Windows 8 security features as defense against cyber security threats. 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 8 Firewall is Enabled**
Device are shipped from the factory with the Windows Firewall on by default. To make sure it hasn't been turned off, follow these steps:

1. Open Windows Firewall by clicking the **Start** button and then clicking the **Search** icon. In the search box, type **firewall**, and then click **Windows Firewall**.
2. In left pane, click **Turn Windows Firewall On or Off**. If prompted for an administrator password or confirmation, type password or provide confirmation.
3. Below each network location type, click **Turn On Windows Firewall**, and then click **OK**. It is recommend that the firewall be turned on for all network location types.

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

③ **Verify Automatic Updating for Windows 8 Operating System Enabled**
With automatic updating, the Operator doesn't have to search for updates online or worry that critical fixes or device drivers for Windows might be missing from the system. Windows Update automatically installs important updates as they become available. The Operator can also set Windows Update to install recommended updates automatically or to inform the Operator that they're available. The Operator can also choose whether to turn on Microsoft Update, which delivers updates for other Microsoft products. Optional updates, such as language packs and updates from Microsoft Update, aren't installed automatically. Windows Update won't add any apps to the system without prompting for permission.

To turn on automatic updating:

1. Open Windows Update by swiping in from the right edge of the screen (or, if using a mouse, pointing to the lower-right corner of the screen and moving the mouse pointer up), tapping or clicking **Settings**, tapping or clicking **Control Panel**, and then tapping or clicking **Windows Update**.
2. Tap or click **Change Settings**.
3. Under **Important updates**, choose the option that you want.
4. Under **Recommended updates**, select the **Give me recommended updates the same way I receive important updates** check box, and then click **Apply**.

IMPORTANT: In order for automatic Windows Update to function, the device must be continuously connected to the Internet. If the device is not connected, Windows updates will need to be performed manually. To do so, regularly go to Windows Update per step 1 above and then click Check and Install Updates button.

④ **Install Windows 8 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.