Recommendation and Guidelines for Medtech Evolution

Medtech Evolution Systems Requirements Specification Guide

Refer to the Medtech Evolution System Requirements Specification Guide and ensure you meet at least Minimum or preferably Recommended Server Configuration.
http://www.medtechglobal.com/nz/support-nz/hardware-specifications-nz/

Install Antivirus, Anti Malware and Anti Spyware protection on every device on your network. A virus scanner is critical; however, Anti Malware and Anti Spyware help provide extra protection. Ensure these are regularly updated, and notifications are configured and monitored.

Always use a Firewall

- A Firewall must be maintained at the perimeter of your network. It is advisable for best security, to have all incoming traffic blocked, with exceptions to allow required traffic only. For greater security, outbound traffic should also be restricted (again only allowing specific ports).
- A Firewall should also be used on all PC's and Servers within your network (either Windows Firewall, or third-party firewall, some Virus Scanners come with integrated Firewall options).
- Refer to Microsoft website for more detail regarding local Windows Firewall configuration or to the relevant Anti-Virus vendor.

Keep your Operating Systems and Software up to date

- For Servers it is advisable to update at least monthly, however for desktops a weekly or on demand patching routine is advised to ensure systems are as secure as possible. Critical security updates may be reviewed and pushed out immediately if the risk is deemed critical and applicable. https://www.cert.govt.nz/it-specialists/critical-controls/patching/creating-a-standard-patchingprocess/
- A comprehensive list of applications should be maintained (including Medtech Evolution, Microsoft SQL Server, Office, and any other third-party applications you may have), and these should be updated regularly, including security updates as they become available. Medtech Applications should be updated when new versions are released.

Backup all data. Ensure all data is stored in appropriate network locations and that these locations are covered by a regular backup process. Medtech Applications & Databases should be regularly backed up, along with any other company data using a daily routine.
Please refer to the Database Maintenance Guide for Medtech Evolution Maintenance and Backup & Restore processes: http://www.medtechglobal.com/nz/support-nz/hardware-specifications-nz/ It is also advisable to test your backup and restore routines regularly.

User Security. Ensure users have their own Accounts and Complex passwords are enforced, with expiry configured.

- Passwords should be at least eight characters in length.
- Should contain a combination of upper- and lower-case letters
- Include at least one numeric and /or special character (& or ? or @, etc.).
- Passwords should have a regular expiry set (30-60 days)

(Further guidelines in HISO document - link at the end of document)
It is also advisable to configure and enforce password policies within the Medtech Evolution system configuration.

User Access Restriction: Lock down all company data to only the required users, lock down all shares and folders appropriately. https://www.cert.govt.nz/it-specialists/critical-controls/principle-of-leastprivilege/

Wireless Security. Ensure complex passwords are used to secure your Wi-Fi network. Apply firmware and security updates, as they become available for your Hardware.

Separate internal users from guest users

Unless your guest users absolutely require access to internal resources, make sure you place them on a completely separate guest Wi-Fi network. All of today's modern enterprise Wi-Fi architectures offer an easy way to safely onboard guest users and segregate them so they only have access to the Internet, not internal resources.

Don't broadcast the name of your wireless network

The name of your wireless network, known as the SSID, should not be broadcast to passers-by. In addition, choose an obscure hard-to-guess SSID name to make life harder for Wi-Fi hackers. SSIDs such as 'home', 'wireless' or 'internet' are not good choices.

Use MAC address filtering

Wi-Fi routers and access points normally can prevent unknown wireless devices from connecting to the network. This works by comparing the MAC address of the device trying to connect to the Wi-Fi router with a list held by the router. Unfortunately, this feature is normally turned off when the router is shipped because it requires some effort to set up properly. By enabling this feature, and only telling the router the MAC address of wireless devices in your household, you'll be securing your wireless network against neighbours stealing your internet connection.
Securing your wireless network using MAC address filtering is not a total solution as it is possible for a determined hacker to clone MAC addresses and connect to your Wi-Fi network, but this measure should still be taken to reduce the risks.

WPA2

Wi-Fi Protected Access 2 -- typically referred to as WPA2 -- is a security protocol that incorporates all of the necessary security elements found in the 802.11i IEEE security specification. There are two different types of WPA2. The first one (WPA2 Personal) uses a standard pre-shared key and the second (WPA2 Enterprise) utilizes 802.1x authentication. If possible, use WPA2 Enterprise whenever possible since it requires each to authenticate using his or her own unique username/password.

Physically secure your APs

Because a wireless LAN must be deployed in a distributed manner, you end up with wireless access points in closets and ceiling throughout a building. Do your best to physical secure the APs to prevent against theft or tampering. Most enterprise-class APs give you the ability to mount and then lock the device in place. Also make sure that any local access to the WAP requires a unique password. **Limit Wi-Fi signal**

When it comes to Wi-Fi signal strength, more is not always better. From a security standpoint, your goal should be to provide sufficient Wi-Fi signal only to the areas where it's required. If you have Wi-Fi signal that reaches beyond building walls and out into public spaces, you risk inviting people who may attempt to break into the network or interfere with the wireless signal.

Wireless intrusion prevention systems

Advanced enterprise wireless security can include a dedicated wireless IPS. These devices monitor and detect more targeted and nefarious WLAN attacks that use techniques such as AP spoofing, malicious broadcasts, and packet floods.

Mobile device management

MDM isn't simply about being able to better manage BYOD devices; there's a security element involved as well. With most MDM solutions, you have the ability to quarantine devices that don't meet set security standards, limit application installations, and implement data loss prevention (DLP) through techniques such as geofencing.

Support legacy Wi-Fi devices

Wireless printers and Wi-Fi-capable handheld scanners are notorious for sticking around for years in the enterprise. In situations where devices don't have the ability to use the most secure form of Wi-Fi authentication and encryption, it's best to segment these devices onto their own separate virtual network with their own unique SSID.

Restrict internet access to certain hours

Some wireless routers allow you to restrict internet access to certain times of the day. For instance, if you know you will not need to access the internet, then schedule your router to disable access between those hours.

More Information is available at the following sources:

Subscribe to Cert NZ for regular threat advisories:
https://www.cert.govt.nz/

Cert NZ regularly publish articles to assist with planning:
https://www.cert.govt.nz/it-specialists/critical-controls/

Health Information Security Framework:
https://www.health.govt.nz/