



KONICA MINOLTA MEDICAL IMAGING Medical Products Virus Protection Policy

JUNE 1, 2004

At Konica Minolta Medical Imaging USA, Inc. (KMMI) our goal is to help protect KMMI products from malicious software attacks, as well as to assist our customers in the event an attack on KMMI products does occur. While healthcare facilities are responsible for providing maximum security on their network infrastructure, KMMI assists our customers to correct any immediate problem until a security patch becomes available.

KMMI takes the following preventive measures to minimize its medical products' exposure to malicious virus attack:

- Provide password protection that limits system access to authorized users only.
- Configure the operating system services that minimize system exposures.
- Validate and approve security patches for installation on KMMI products. Due to rigorous regulatory requirements and KMMI quality and performance standards, each patch is subject to extensive testing and validation prior to becoming approved for installation on KMMI products. Only KMMI approved patches may be installed on KMMI products.
- Install approved security patches during scheduled preventive maintenance visits for products covered under warranty or service contracts. For out-of-warranty, non-contract products, KMMI will install security patches per KMMI service billing schedule.

In the event a security attack occurs at the healthcare facility's network, and consequently on KMMI products, please contact KMMI customer support immediately for assistance (1-800-945-0456). Once KMMI customer support confirms the virus attack, a qualified KMMI service engineer will be dispatched to the site to repair virus infections and restore the systems to working condition. **This is a billable service to all KMMI customers.** Installation of non-Konica approved patches or installation by non-KMMI certified personnel on KMMI products may render product warranty invalid. Furthermore, while anti-virus software provides security for a system connected to a network, it is not advisable for installation on medical devices. Installing anti-virus software on KMMI products may compromise performance and may render product warranty invalid.

To optimize a network system's security from virus attack, consider employing the following practices:

- Use technical network defenses, such as firewalls, network virus scanners, intrusion detection systems, audit records, and VLANs.
- Prepare policies, procedures, and user training (i.e. safe practices while on an intranet)
- Restrict physical access whenever possible
- Establish secure remote access for servicing, such as Secure VPN.
- Notify the appropriate vendor in the event of a virus attack. Disconnect the device from the network to avoid spreading the virus to other devices.

Each facility must evaluate its local requirements and use every measure possible to increase the level of protection against the threats imposed by a malicious virus. KMMI will support our customers to resolve all virus-related problems that impact the performance of our equipment. Thank you and we appreciate your support of Konica Minolta Medical Imaging products.