



**Polycom iPower Security FAQs**  
**October, 2002**



### iPower Security Frequently Asked Questions

The FAQ addresses questions about how unauthorized access, and network-and application-based viruses may affect iPower systems. It covers what you need to know about how the systems work, and suggests proper management procedures and appropriate policies for security.

Technology, by definition, is constantly moving and changing. We strive to adopt these changes quickly to deliver higher efficiencies and productivity in the workplace. Polycom is at the forefront in delivering innovations based on the standards and platforms used most widely in enterprises today. Although in today's environment there is no such thing as a perfect technology solution, the value and benefits that these solutions provide far outweigh potential risks.

iPower systems use Microsoft's Windows operating system. This allows us to take advantage of the considerable work done globally to make computers secure and allows your IT department to use the knowledge and practices they have already developed for your company's PCs. No one seriously suggests that the world do without PCs because of potential security risks. Instead, measured steps are taken to provide and enhance security while preserving the tremendous increases in productivity and effectiveness brought by having real time access to information. The same considerations apply to security steps for iPower systems.

This document contains general information about Polycom iPower systems and security. If you need specific information and recommendations on security issues, including protection against Internet- and application-based viruses, please refer to the Security Center of the Polycom Web-site.

#### **Q. Are iPower systems vulnerable to viruses and other security attacks?**

A. *Just like other network and computing devices, such as PCs, router, cell phones and PDAs, iPower systems can be subjected to security attacks. The risks are dependent on how the systems are connected to the network and how people use them. If an iPower system is connected to ISDN lines, without internet access and user access to media drives and applications disabled, they are no more of a security risk than an appliance video conferencing system.*

#### **Q. How do I protect an iPower System?**

A. *Polycom iPower systems are based on Microsoft Windows 2000 and protection should be handled in the same way that you treat any other PC. This includes, for example:*

- *Restricting access to authorized users by using appropriate passwords*
- *Installing anti virus software and ensuring that floppies or CDs are scanned before using*
- *Keeping your anti-virus software updated – just as you do with any other PC in your organization*
- *Using the Windows Device Manager to disable access to the floppy and CD-ROM, if this is your policy*
- *If your system is connected to the LAN, using the same procedures that are in place to provide security for any other PC on the LAN. Typically, this includes taking the steps above plus providing Firewall protection.*
- *Installing relevant Microsoft Window security patches as they become available*

#### **Q. Are other video conferencing systems vulnerable?**

A. *Other video conferencing systems have operating systems, just like a computer. They may also have other components such as a web server for remote access, management or presentations. Any of these components can be the target of a virus. In the recent past, viruses have successfully attacked even unexpected appliances such as routers and cell phones. Since some other video conferencing systems do not use operating systems as widely accepted as Microsoft Windows or do not expose the operating system to the user, security support may only be available from the appliance vendor.*



## Polycom iPower Security Frequently Asked Questions

October, 2002

**Q. Can an infected file be loaded onto my iPower system? How can I prevent this?**

A. *There are several ways to limit the risk of infection. The simplest is to install and maintain anti-virus software. Also, if a system is not physically connected to the LAN, there is no risk of accessing bad files on the network (but this also means there is no access to important data stored on the network). An iPower system can also be set to boot up automatically to the video application and, by setting low level user password rights, the administrator can prevent routine users from accessing other applications. Similarly, from within Windows, both the floppy and CD-ROM can be disabled to ensure no other applications can be loaded. Whatever steps are taken, an important advantage remains; the full power of iPower systems' collaboration capabilities are available whenever you need them, simply by changing user privileges and connection arrangements.*

**Q. How can I protect against Internet-based viruses and unauthorized access?**

A. *Most organizations protect their local area networks from Internet viruses and unauthorized access by maintaining an adequate Firewall. iPower systems connected to the LAN are also protected by this Firewall. Anti-virus software is highly recommended.*

**Q. I have an iPower system connected via ISDN only. Can people get access to my corporate data?**

A. *No - if you have no LAN connection there is no physical means to get access to that information.*

**Q. I am connected to the LAN, but use ISDN to make video calls. Can people get access to corporate information?**

A. *When you make an H.320 ISDN connection you are making a video call. There is no mechanism in H.320 that allows parties in the call to gain access to the LAN.*

**Q. If I make an IP video call over an external network does the remote user have access to the system and thus our corporate LAN?**

A. *As with any IP traffic that is external you should ensure that you have a Firewall that provides adequate security and protects the identity of your system. The same is true for anyone who uses a browser to download or access information on the internet. There is no mechanism within H.323 IP video calls that allows a participant to gain access to the LAN.*

**Q. When T.120 data sharing is enabled, does that allow the far end to control your PC?**

A. *T.120 datasharing allows you to share (allow the far end to view) an application or to give the far end control of an application that you wish them to control. The far end cannot view or control an application without you allowing them to do so.*

**Q. Can someone "listen in" to an H.320 ISDN call?**

A. *Eavesdropping on the audio portion of an H.320 call is about as difficult as eavesdropping on a standard telephone call. Since a typical video call uses 6 separate connections across the network, viewing the entire conference is considerably more difficult: an eavesdropper would need to access all 6 channels and adjust the delay between them. Customers do have the option to encrypt calls for even more security.*

**Q. Can someone access the LAN via RAS on an iPower system?**

A. *As default, Polycom iPower systems have RAS disabled. If you wish you can configure remote access on one of the ISDN channels – assuming you want to manage those systems remotely and do not have access via the LAN. Under Windows 2000 you can select whether that will allow access to only the iPower system or to the entire network.*



## Polycom iPower Security Frequently Asked Questions

October, 2002

**Q. Different users use the system. How can I prevent them gaining access to certain PC applications?**

*A. User profiles can be set up to restrict access to any PC application.*

### Summary

Polycom iPower systems offer high levels of security because they are standards-based and designed to take advantage of all the standard security features already in place within an organization. These include User Privileges, Proxy Servers, Firewalls, RAS connections, Anti-Virus software etc. – basically the same security tools that are used in the most widespread and most sensitive business applications. Users are more comfortable with familiar approaches and can apply consistent policies and procedures to iPower systems, PC's and Servers alike. Even in comparison to appliance video systems with proprietary Operating Systems, iPower collaboration systems fit well into the customer's existing infrastructure.