

# Using Instant Medical History™ in a Secure Environment

Copyright 2003-2006, Primetime Medical Software, Inc.

## ***Disclaimer and notice of limited liability***

Primetime Medical Software (hereinafter “Primetime”) has produced this document for the exclusive use of Primetime customers using Instant Medical History™. No other use of the information contained in this document is intended or permitted. Primetime has exercised reasonable care in testing the procedures documented herein. Since computer security requires that the user examine all possible avenues for breach of security, and since Primetime does not and cannot address all possible breaches of security, Primetime accepts no responsibility for breaches of security that result after following the procedures contained in this document. The user accepts that responsibility for security of computer systems resides solely with the user and consultants to the user who contractually agree to accept such responsibility. Primetime’s sole responsibility is to correct any procedural or grammatical errors contained herein upon written notice of such errors by Primetime customers.

No warranty is made or implied for suitability of the procedures contained herein to meet the requirements of any regulatory or governmental agency. Primetime believes that implementation of these procedures will provide security and confidentiality needed to meet the expectations of agencies charged with administering provisions of law designed to protect patient confidentiality and security. No verification has been sought or received by Primetime that this is in fact the case, and no representation is made by Primetime to the effect that these procedures meet the requirements of any law, regulation, governmental or regulatory agency.

## ***Important Notice***

The procedures outlined in this document have been tested with the software discussed and found to work as described. However, there are many steps involved in carrying out these changes, and it takes some time to complete each step in the process. Be sure that you clearly understand the directions before you proceed. If you encounter a situation that looks different from that described in these directions, stop and call Primetime Software for help. Do not attempt to proceed if you are unsure about what you are seeing on your computer or do not understand the directions. It is possible that you could damage your computer or lose any data, or disrupt normal operation of your computer for some period of time if you make mistakes while implementing these changes. You should also be well rested and alert before starting to make these changes, and preferably should work with someone who can read you directions and help you keep your place in the directions.

If you have any doubts about your ability to carry out these directions, you should consider contracting the work out to a qualified person. The procedures outlined in this document may require special understanding or technical expertise beyond that of a

competent user of Windows™ products. It is possible however to get into some functions of your computer that can disrupt normal functions and require special assistance to resolve.

## ***Preface***

This document is a supplement to the manuals and help files associated with Windows 2000™, Windows XP Professional™, and Windows NT™. It is not intended to replace the information in the documentation supplied with your operating system, but rather specifies how to set some of the options that your operating system contains. The author assumes that the reader has a certain level of familiarity with the installation and operation of Windows™. If you are having difficulty with any of the sections in this document, we would be happy to assist you to the extent that our instructions are unclear. However, if you need significant additional help understanding the operation and implementation of your version of Windows™, please contact us to arrange for our value added consulting services. Similarly, if you need assistance configuring or installing network components to comply with security standards or your own particular needs, we would be happy to discuss providing those services.

## ***Introduction***

Instant Medical History™ is an application that allows patients to complete questionnaires about their medical concerns, and stores the results of these questionnaires in an electronic form. The law requires that physicians take responsibility for the security and confidentiality of medical records produced under their guidance, and the output of Instant Medical History is a part of the medical record. This document outlines the steps that you need to take to meet your obligation for keeping the output from Instant Medical History™ secure and confidential.

Each time that Instant Medical History™ runs a questionnaire, the output is stored in two forms. If you have chosen to use Instant Medical History™ with an electronic medical record program, there may be a third (optional) type of stored output form.

The first form is the original data form. The file for the original data will have an “IMH” extension. The default location for these files is C:\Program Files\Primetime Medical Software\Primetime Instant Medical History\Screenings\Original. Your files may be stored in a different location if during setup you chose another location for your copy of Instant Medical History™.

The second form is the word processing text file that is saved after you have reviewed the output. This file will have an extension that depends upon the file type you have chosen when you set up Instant Medical History™. This could be a .DOC extension for Microsoft Word™ format, a .WRI extension for Rich Text format, a .TXT extension for text, or an .HTM extension for HTML format. This second form may be saved in two different locations, depending upon options that you select when you install Instant Medical History™. Use the Tools\Options\Report Preview\Report Preview Output Locations option to see

what location or locations (Primary and Secondary) have been selected for storing the word processing output file for your computer. **WARNING!** Each time you review a word processing document produced by Instant Medical History™, you have the option of saving that document in a different location. If you choose to save these files in a new location, you must also apply the security settings below to that location in addition to the locations described. Otherwise you may produce unprotected copies of patient records.

The third output form is the form required by your electronic medical record. If you do not have an electronic medical record and have not set up your copies of Instant Medical History™ to produce output destined for an electronic medical record, you do not need to concern yourself with this third form. If you have designated output to be sent to an electronic medical record, use the Tools\Options\EMR\EMR Output Location option to see what location has been selected for storing the EMR output file on your computer.

For your computer to be compliant with security and confidentiality regulations, all of the locations that you use to store the output of Instant Medical History™ must be protected from unauthorized access. Unauthorized access means access by anyone in your office who is not your employee AND is not normally allowed access to such records in the course of his/her normal functions for providing patient care within your office. Instant Medical History will create a log of each time the Instant Medical History menu is used to Open, Print, Manage, and Delete a file.

In the next sections, we will describe the steps you need to take to make your files inaccessible to unauthorized users.

### ***Operating systems***

Instant Medical History™ will work correctly with Windows™ 2000, Windows NT 4.0, and Windows XP Professional. **The only operating systems that provide the underlying security features needed for compliance with security and confidentiality requirements are Windows NT™ 4.0 and Windows™ 2000/Windows XP Professional Version.** Therefore, you must be certain that you are running Instant Medical History™ only on computers that use either Windows NT™ 4.0, Windows XP Professional, or Windows™ 2000 Professional as the operating system. **Other versions of Windows will run Instant Medical History™ properly, but will not provide the necessary password protection and file security needed to be in compliance with expectations for security.**

Windows NT™ 4.0 and Windows™ 2000 must be installed using the NTFS as its file system for the necessary security features to be enabled. **Using the FAT or FAT32 file system will not allow you to set the security privileges in a way that will keep your patient information files protected from unauthorized access.** You must be sure that NTFS is the file system on the drive that your patient information from Instant Medical History™ will be stored. If you attempt to follow the directions below on a drive that is formatted using the FAT or FAT32 file system, you will be unsuccessful.

**For Windows NT 4.0™:** If you are unsure what file system your computer is using, first log into Windows™ NT as an administrator. Run the Disk Administrator program (Start menu /Programs / Administrative Tools/ Disk Administrator). Find the line with the drive letter that matches the drive you will be using to store your output from Instant Medical History™. The line that describes the disk will contain the disk name (C: etc), the amount of storage space on the disk, and the file system type (NTFS, FAT32 or FAT). If the drive you are going to use is NTFS, you are ready to go to the next step. If not, you must first convert the drive you wish to use to NTFS. Windows NT™ can do this for you without reformatting your drive or losing any data.

**For Windows 2000(TM)™:** If you are unsure what file system your computer is using, first log into Windows™ 2000 as an administrator. Start the Control Panel (Click the Start button, then click on Settings, then on Control Panel). When Control Panel is running, double click on the Administrative Tools icon. Administrative Tools opens a window with a number of additional icons. Click on the Computer Management icon. In the Computer Management window double click on the Disk Management icon. This will bring up a list of the drives on your computer. Find the box with the drive letter that matches the drive you will be using to store your output from Instant Medical History™. The box that describes the disk will contain the disk name (C: etc), the amount of storage space on the disk, and the file system type (NTFS, FAT32 or FAT). If the drive you are going to use is NTFS, you are ready to go to the next step. If not, you must first convert the drive you wish to use to NTFS. Windows™ 2000 can do this for you without reformatting your drive or losing any data.

#### **If you need to convert a drive to NTFS...**

Your Windows™ 2000 installation manual has complete instructions for converting a drive format to NTFS. These instructions will not be duplicated here. Be certain to read and follow these directions carefully. The process is fairly straightforward, but you should back up the drive you are converting before you begin the conversion process.

Regardless of which operating system you use, there are several important points to consider when using computers in your office.

1. Be sure that all computers that contain patient information or access a network on which patient information is available are running a secure operating system.
2. Limit the amount of time that patients can have access to a computer without some supervision by your staff.
3. If patients will have extensive access to computers without supervision, you may wish to consider third-party desktop security programs to restrict access to programs.
4. If your local area network also connects to the Internet, be sure that you have a firewall between your local network and the Internet.
5. If you are using any wireless devices in your network, encrypt all transmissions.
6. Keep an audit trail of all log on access and all file access of files containing patient information, so that you can document your compliance to regulatory agencies.

7. Give each of your staff members their own unique log on name and password for access to your computer systems. Log on names should be difficult to guess. Passwords should be complex, and contain a combination of letters and numbers. Prohibit sharing of log on names and passwords among your staff.
8. When a staff member leaves your employment, delete his/her log on name from your system. Set your security so that the same log on name cannot be re-used to prevent confusion in your audit trail.
9. Be sure that all staff members are trained to log off from their computers whenever their computers are unattended. Periodically audit compliance with this practice, and document that you have audited compliance.
10. Restrict the number of users who have high level or administrative access to your systems.
11. Restrict the printing of patient information to those staff members trained to handle the printed documents in a way that is compliant with confidentiality restrictions.
12. Use e-mail for the transmission of patient information only over a secure link, and only send information that is encrypted. Document all instances of e-mail transmission of information, and compliance with encryption and secure messaging.
13. Designate a person in your office who is the "Security Manager". This person should be entrusted with the access to passwords for all users so that lost passwords, new users, and terminated employees can be dealt with through a single source. The Security Manager should also be responsible for training your staff about confidentiality and security issues in your office.

This should not be considered an exhaustive list. It should be used as a general starting point.

### ***Setting security options in Instant Medical History™***

The first step in establishing the security of your system is to set a password within Instant Medical History™ that limits your patient's options for "exploring" the menu functions and prevents your patients from exiting the program or minimizing the program window. This is done with Instant Medical History™ running. Click the **Tools** section on the menu bar, then click **Options** from the drop down menu. You will see seven tabs across the top of the Options window. Click on the **Passwords** tab.

#### The Passwords Tab

The Passwords tab has two different areas for customization. There are two rectangular boxes that work in tandem to define the function of passwords in Instant Medical History™. The box on the right sets the application password, the box on the left sets the functions of the application password.

## The Application password

A password can be set to restrict certain normal program functions to qualified personnel. Each copy of Instant Medical History™ that you run in your office can have a different password if you like, or they can all be the same. Once you choose a password and type it into the box labeled Password, you must type the identical password in the box labeled Confirm Password. This is done to protect you from accidental typographical errors that could prevent you from using the software. Note that when you type a password, what you type does not appear in the box but that each character you type is replaced by an asterisk (\*) character. This is to keep anyone from seeing what you have typed in this box. Since it also makes typographical errors impossible to see, the Confirm Password box helps to protect you from accidentally typing something you did not mean to. Set your password now.

Once you have entered a password, the four check boxes on the upper left-hand box will control where the password is required:

Checking the top box, Close the application, (by clicking on the box) will require that you type the password each time you try to exit from Instant Medical History™. This will be true however you try to exit from the program. This is useful for keeping patients from accidentally closing the software and requiring your staff's time to re-start it for the next patient. This box should be checked.

Checking the upper middle box, View screening output, (by clicking on the box) will require the password to view any output file that Instant Medical History™ has produced. This protects the confidentiality of your patients. Note however that if you save your Instant Medical History™ output as a text file that can be accessed by a word processor, this password will not provide any protection. **This password will only prevent unauthorized access to files using Instant Medical History™, but not access gained directly to files by use of a word processor or through the operating system.** Additional steps are defined below to prevent access to files by these other means. This box should be checked.

Checking the lower middle box, Access Application Options, (by clicking on the box) will require the password to get back to the Options window. Enabling password protection will prevent unauthorized users from changing your options. This box should be checked.

Checking the bottom, Exit Screening Wizard, (by clicking on the box) will require the password to exit the screening wizard if you run IMH in this mode. This box should be checked.

If you lose or forget your password, there you must call Primetime Software for instructions on resetting your password. We will give you detailed instructions once we verify your need to reset the password

Next click on the General tab. In the “Other settings” box, there are seven check boxes. Check the bottom box labeled “Only run the application maximized (disables minimize and restore)”. Now click OK.

You may now exit Instant Medical History™. If you have set things up properly, you should be required to enter your password to exit from the program. The minimize window button should no longer be visible.

### ***Setting up a new user logon with limited privileges.***

The first step in securing your system is to create a simple log in for patients that requires no training or staff intervention. The process outlined in this section creates a new user on your computer named “patient”. When this user logs in, no password is required. This user will have very restricted access to the computer, which will protect certain directories and files from unauthorized access and unwanted meddling. You must be logged in as an administrator to begin this process.

## **Windows NT™ 4.0 users begin here:**

### **Step 1**

Start User Manger (Start / Programs/ Administrative Tools / User Manager).

Click on User, then select “New User” from the drop down menu.

Create a new user with the Username of “patient”. Leave the Full Name, Description, and Password sections blank. Uncheck the “User Must Change Password at Next Logon” box. Check the “User Cannot Change Password” box and the “Password Never Expires” box.

Click on the “Groups” button at the bottom. This should bring up a dialog box, with the group “Users” in the box labeled “Member of:”. Be sure that “Users” is the ONLY group that patient is a member of.

Click OK. This returns you to the New User Window.

Click OK again.

Click on the “Policies” drop down from the User Manager Menu, then click on “Account Policy”. Make sure that “Permit Blank Password” is selected.

Click OK.

Exit from User Manager.

This will allow “patient” to log on without entering a password, simplifying the logon process for your patients.

### **Step2**

Log off as an administrator (Start / Shutdown/ Close all programs and log on as a different user).

Log on as “patient”. Then log off again, and log back on as the administrator (this is necessary to create a profile folder for the user “patient”).

Go to the desktop. Double click on “My Computer”

Double click on the “C:” drive icon.

Double click on the “Winnt” folder

Double click on the “Profiles” folder

Double click on the “Patient” folder

Double click on the “Start Menu” Folder

Double click on the “Programs” folder

Double click on the “Startup” folder

Single right click with the cursor in the Startup window. This will bring up a dropdown menu. Click on “New”, then “Shortcut”. On the “Create Shortcut” box that opens, click the “Browse” button. Double click on “Program Files”, then double click on “Primetime Medical Software”, then double click on “Primetime Instant Medical History”, then double click on the icon next to IMH.EXE. Click the Next button. Click the Finish button. Close the window.

You have now set your computer up so that when someone logs in as “patient”, Instant Medical History™ will automatically run.

### **Step 3**

Go to the desktop. Double click on “My Computer”, then double click on C:

**If you have installed your copy of Instant Medical History™ on a drive or directory other than the default drive and directory, you will need to modify the instructions that follow to account for the location of your program and data.**

Double click on Program Files. Double Click on Primetime Medical Software. Double click on Primetime Instant Medical History. Single right click on Screenings. Single click on Properties. This should open a dialog box labeled Screening Properties, with three tabs across the top labeled General, Sharing, and Security. **(If only two tabs are present, your drive is not formatted as NTFS. Please re-read the section titled Operating Systems again. You will not be able to proceed with the remainder of this process until your drive is formatted using NTFS).**

Click the Security Tab.

Click the Permissions button. This opens the Directory Permissions window.

Check the box labeled Replace Permissions on Subdirectories. Check the box labeled Replace Permissions on Existing Files.

The large text window labeled Name: should say “Everyone ...Full Control [All][All]. Single click on Everyone, then click on the Remove button. The Name: window should now be empty.

Click the Add... button. This opens the Add Users and Groups dialog box. Double click Administrators from the Names: window. This should add Administrators to the Add

Names: window at the bottom. Open the Type of Access: box at the bottom, then click Full Control. Click OK. The Directory Permissions box should now have an entry for Administrators with Full Control

Click the Add... button. This opens the Add Users and Groups dialog box. Click the Show Users button. Scroll down the Names: window until you find the entry for patient. Double click on patient. This should add patient to the Add Names: box. Open the drop down list in the Type of Access dialog box. Click on Add, then click OK. The Directory Permissions box should again appear, this time with two entries. The patient entry should have Add[WX][Not Specified]. Click OK.

When asked "Do you want to replace the security information on all existing subdirectories...", click Yes.

Leave the Properties window open for now and go to Step 4.

Step 3 has reset the permissions on the directory that Instant Medical History™ uses to store its output, allowing patients to create new records, but not to read or change any existing records. However, if you have set up additional (optional) directories for Instant Medical History™ output, you will need to repeat step 3 on **each** directory where output is stored. See the section above titled Introduction for a more complete description of how to set options for storage of output for Instant Medical History™.

**If you make copies of any output files from Instant Medical History™ and store them on your computer, you should use this same process to secure ALL directories where you store these output files. Instant Medical History™ cannot control what you do with patient records after their creation. For your own protection, it is essential that you control access to any directory on your computer that may contain patient information.**

#### **Step 4**

Click on the Auditing button. This opens the Directory Auditing window. Check on the Replace Auditing on Subdirectories box. Check the "Replace Auditing on Existing Files" box.

Click the "Add..." button.

Double click Administrators.

Click the "Show Users" button

Double click patient in the users box

Click OK to return to the Directory Auditing window.

Check the Success and Failure boxes for Read and Write (4 boxes)

Click OK

**[If auditing access has not been enabled, you may need to run User Manager again to enable auditing. Check your Windows NT™ manual or the online help file to learn how to enable auditing.]**

You have now enabled an audit trail for creation of and access of your patient records files.

If you need to give any of your staff members access to clinical files, we suggest that you use additional security features to create special user logon names for each staff member in your office, with appropriate levels of privilege for their required use of the files. We also suggest that you keep a log of all access made to patient records by your staff members. In the event of an audit, you will then be able to account for all access to patient files. These setup options are beyond the scope of this document. We would be glad to discuss any additional assistance you may require.

### **Step 5**

Log out of Windows, then log back in as “patient”. Press the Windows key (located between the Alt and the Ctrl key). Click on “Start” then “Settings” then “Taskbar & Start Menu”. Uncheck the box next to Always on top. Uncheck the box labeled “Autohide”. Click the “Advanced” tab. Examine the list of programs on the Start menu, and remove any that you do not want the user “patient” to have access to. Click OK

### **Step 6 (Optional)**

What you have done up to this step will protect your patient data files. It is possible to control access to all of your program files and other data files as well. If you are interested in further protection for your computer, please contact us for a quote on consulting services to accomplish this higher level of protection.

## **Windows 2000™ / XP Professional users begin here:**

### **Step 1**

Start the Control Panel (Start / Settings / Control Panel). Click on Users and Passwords. Click the “Add...” button on the Users tab. Enter the User name of “patient”. Leave the Full name and Description fields blank. Click Next. Leave the Password and Confirm Password fields blank. Click Next. Click the Restricted user radio button. Click Finish. Click OK to exit the Users and Passwords utility.

Now double click on “Administrative Tools”. Double click on “Local Security Policy”. Double click on “Account Policies”. Double click on “Password Policies”. Set “Minimum password length” to 0 (zero) characters.

Click on the “Local policies” folder in the left pane. Click on “Audit policy”. Double click on “Audit object access”. Be sure that the “Success” and “Failure” boxes are checked. Click OK. Exit from “Local security settings”.

From the “Administrative Tools” window, double click on “Computer Management”. Double click on “Local Users and Groups” in the left pane. Double click on the “Users” folder. Double click on the icon next to “patient” in the right pane. This should bring up a window labeled “patient Properties”, with three tabs at the top Labeled “General”, “Member of” and “Profile”. From the General tab, check the boxes “User cannot change

password” and “Password never expires”. Be sure that the other boxes are unchecked. Click on the “Member of” tab. Make sure that “Users” is the only group in the “Member of: “ window. If any other group is present, click on it, then click the “Remove” button.

Click OK

Close the “Computer Management” window

Close the “Administrative Tools” window.

## **Step 2**

Log out of Windows (Start / Log Off) Now log back in using the name “patient”. Be sure to leave the password screens blank.

Click on “Start” then “Settings” then “Taskbar & Start Menu”. Uncheck the box next to Always on top. Uncheck the box labeled “Autohide”.

Click the “Advanced” tab. In the window labeled “Start menu settings” uncheck all of the boxes.

Now click the “Advanced” button. Double click on the “Programs” menu icon. Remove any programs or folders that you do not wish “patient” to have access to.

Now double click on the “Startup” folder.

Single right click with the cursor in the Startup window. This will bring up a dropdown menu. Click on “New”, then “Shortcut”. On the “Create Shortcut” box that opens, click the “Browse” button. Double click on “Program Files”, then double click on “Primetime Medical Software”, then double click on “Primetime Instant Medical History”, then double click on the icon next to IMH.EXE. Click the Next button. Click the Finish button. Close the window.

Now examine the icons on the desktop. Delete any icons of programs that you do not wish users to have access to. (This will change the desktop for this user only, and should not affect other users with other logon names)

Now log out of Windows (Start / Log Off patient). Log back in using your administrator name and password.

## **Step 3**

Go to the desktop. Double click on “My Computer”, then double click on C:

**If you have installed your copy of Instant Medical History™ on a drive or directory other than the default drive and directory, you will need to modify the instructions that follow to account for the location of your program and data.**

Double click on Program Files.

Click on “Show Files”.

Double Click on Primetime Medical Software. Double click on Primetime Instant Medical History. Single right click on Screenings. Single click on Properties. This should open a dialog box labeled Screening Properties, with three tabs across the top labeled General, Sharing, and Security. **(If only two tabs are present, your drive is not formatted as NTFS. Please re-read the section titled Operating Systems again. You will not be able to proceed with the remainder of this process until your drive is formatted using NTFS).**

Click the Security Tab.

Uncheck the box labeled “Allow inheritable permissions from parent to propagate to this object”. You will get a warning message “You are preventing any inheritable permissions from propagating to this object. What do you want to do?” Click the “Remove” button. This will empty the Name window of all users.

Click “Add...”. Double click the individual users you wish to give access to the files in this folder. As you double click each one, it will be added to the lower text window.

When you are finished adding names, click the “OK” button.

You can now set permissions for each of the users that are in the “Name” window at the top of the Screenings Properties window.

Click on “patient”. In the “Permissions” window, check the “Write” box in the “Allow” column, and uncheck all other boxes in the “Allow” column. In the “Deny” column, check the “List Folder Contents” and “Read” boxes. **DO NOT CHECK THE READ AND EXECUTE BOX IN THE “DENY” COLUMN!**

Set permissions for the other users in your list. See the Windows™ documentation if you are unsure how to do this for your other users.

When you are done setting permissions, click the “Apply” button. You will receive a warning that Deny entries take priority over Allow entries. Click “Yes” to continue.

Now click the “Advanced...” button. Click the “Auditing” tab at the top of the window. Click the “Add...” button, then double click on “Everyone”. Click on “Everyone”, then click “View/Edit...” Check the “Successful” and “Failed” boxes for the “List Folder/Read Data” row. Click OK.

Then click “OK” again to return to the “Screening Properties” window.

Click OK once again to finish and close all windows.

Step 3 has reset the permissions on the directory that Instant Medical History™ uses to store its output, allowing patients to create new records, but not to read or change any existing records. However, if you have set up additional (optional) directories for Instant Medical History™ output, you will need to repeat step 3 on **each** directory where output is stored. See the section above titled Introduction for a more complete description of how to set options for storage of output for Instant Medical History™.

**If you make copies of any output files from Instant Medical History™ and store them on your computer, you should use this same process to secure ALL directories where you store these output files. Instant Medical History™ cannot control what you do with patient records after their creation. For your own protection, it is essential that you control access to any directory on your computer that may contain patient information.**

You have also enabled an audit trail for creation of and access of your patient records files.

If you need to give any of your staff members access to clinical files, we suggest that you use additional security features to create special user logon names for each staff member in your office, with appropriate levels of privilege for their required use of the files. We also suggest that you keep a log of all access made to patient records by your staff members. In the event of an audit, you will then be able to account for all access to patient files. These setup options are beyond the scope of this document. We would be glad to discuss any additional assistance you may require.

#### **Step 4 (Optional)**

What you have done up to this step will protect your patient data files. It is possible to control access to all of your program files and other data files as well. If you are interested in further protection for your computer, please contact us for a quote on consulting services to accomplish this higher level of protection.

#### ***Using security logs***

The steps above created security logs of access to patient records created with Instant Medical History™. To monitor who is using your files, you need to open the log files and understand how to read them and maintain them. Most of this information is in your Windows™ help files, and will not be duplicated here. The information provided here is simply to get you started and to provide a framework for working with security logs.

Windows NT™ and Windows 2000™ access the security logs differently. The Event Viewer program in NT 4.0 is accessed from the Administrative Tools program menu, while in Windows 2000™ it is accessed from Control Panel/ Administrative Tools. Double click on Event Viewer, then double click on “Security Log” to see the log of events. To look at details of an individual event, double click on the event. Your Windows™ documentation contains information on clearing event logs, saving copies of logs for auditing purposes, and taking old logs off line to save disk space.

#### ***Local area network security***

The steps above create security for files on individual machines. Creating security for your local network is beyond the scope of this document, but follows along the same

general concepts. If you need help with network security, please call us to discuss a consultation regarding your needs.

***Wide area network security***

Security for wide area networks requires consultation with security experts versed in special security issues. We suggest that if you are building a wide area network that you contact a specialized security consultant.