



**Symantec AntiVirus™
Corporate Edition 10.0
Installation Guide**



Symantec, the Symantec logo, Norton AntiVirus and Symantec AntiVirus are U.S. registered trademark of Symantec Corporation.

Copyright © 2005 Symantec Corporation. All rights reserved.

Table of Contents

Table of Contents	ii
Introduction.....	iii
Step 1: Infrastructure Decisions	1
Primary Server and Secondary Servers.....	1
Managed and Unmanaged Clients	1
Design	2
Step 2: Preparing for Installation.....	3
Obtaining Media and Licenses (New Process)	3
Removing Current Antivirus Software	4
Step 3: Installing Symantec System Center and Snap-ins	5
Step 4: Installing and Configuring Definitions Server Software.....	6
Installing Server Software.....	6
Making a Server the Primary Server.....	7
Configuring Your Definitions Source.....	7
Allowing 10.0 Server to Manage 9.x Clients.....	8
Backing up and restoring the pki folder.....	8
Step 5: Installing Windows Clients	9
Step 6: Installing Macintosh Clients	10

Introduction

Thank you very much for your participation in the North Dakota K-12 Computer Virus Protection Plan. This manual is provided to North Dakota K-12 schools to assist them in deploying Norton Antivirus Corporate Edition within their districts.

In order to keep the size to a minimum, this guide does not cover all facets of the Symantec AntiVirus Corporate Edition applications. This information is located in a complete implementation guide, user's guide and installation guide on the CD. If you would like more detailed instructions, please look in the /Docs folder on Disc 1 (Windows Software) of the SAVCE 10 CD media distributed by EduTech.

If you have any questions, please contact the EduTech Help Desk.

The EduTech Support Staff
sendit.helpdesk@sendit.nodak.edu
800.774.1091
PO Box 6154
Fargo, ND 58105-5164

Symantec AntiVirus™ Corporate Edition 10.0

Installation Guide

Step 1: Infrastructure Decisions

Primary Server and Secondary Servers

The **Primary Server** is the machine which will receive antivirus definitions directly from EduTech and deploy them to your school's managed clients (more on those in the next item). Your Primary Server should be running Windows NT 4 Server, Windows 2000 server, or Netware. Note that your Primary Server can continue to fulfill other functions, such as being a file server.

Recommended specifications:

- Windows 2000 Professional/Server/Advanced Server, Windows XP Professional or Windows Server 2003 Web/Standard/Enterprise/Datacenter.*
- 128 MB for SAVCE only, 256 MB or more if running other services
- 100 megabit Ethernet Card (10 megabit is acceptable)
- At least 150 MB free hard disk space

A **Secondary Server** receives its antivirus definitions from the Primary Server and distributes them to AntiVirus clients. It will be unnecessary for most districts to set up a secondary server. A single primary server can manage thousands of clients efficiently over 100Mb LAN connections. However if you have a facility with many managed computers which is connected to your Primary Server via 56k or similar bandwidth you may wish to set up a Secondary Server in that location. That way you only have to push one set of definitions across the slower connection. The secondary server will distribute the definitions within the facility at much higher LAN speeds.

Managed and Unmanaged Clients

You may have two types of installations in your school: Managed and Unmanaged clients. It is recommended that whenever possible, you set up the clients in your district as Managed.

Managed Clients receive their updates directly from their Primary (or Secondary) Server whenever new definitions come out. The Primary/Secondary Server can also view information on managed clients (for example when scans have been done, whether viruses have been found, what action was taken, etc...). The Server may also initiate a scan on a machine it manages. All clients installed on Windows can be set up as Managed Clients.

* NetWare servers are also supported by SAVCE. For information on NetWare requirements, see pg 37 of the SAVCE Implementation Guide (/docs/savinst.pdf on the SAVCE 10 CD)

Unmanaged Clients receive their updates through LiveUpdate on a scheduled basis. You must configure the machine to connect to Symantec’s LiveUpdate server at regular intervals to determine if new definitions are available. These machines are not visible to the Primary/Secondary Servers in your district. DOS, MacOS and OS/2 can only be configured as Unmanaged Clients.

Design

You should now sketch out an outline of your school districts network. This doesn’t have to be anything fancy, simply determine where your district will have managed clients and unmanaged clients and how those machines connect to the internet. Examples are shown below.

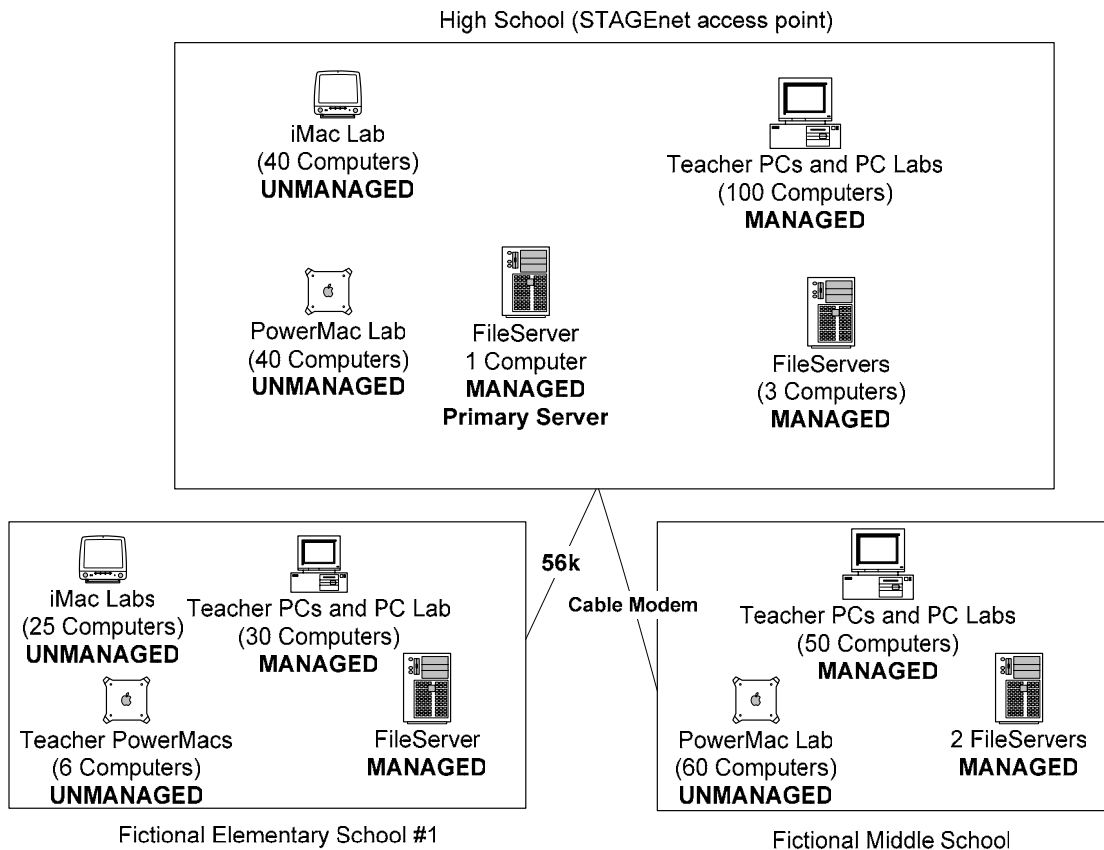


Figure 1 A rough map of Managed and Unmanaged clients in the district along with their inter-district network connection.

Sketches will help you determine if you will need secondary servers at any location. If you have a large number of managed computers (more than 50) with a slow network connection to your primary server, you may want to set up a secondary server at that location.

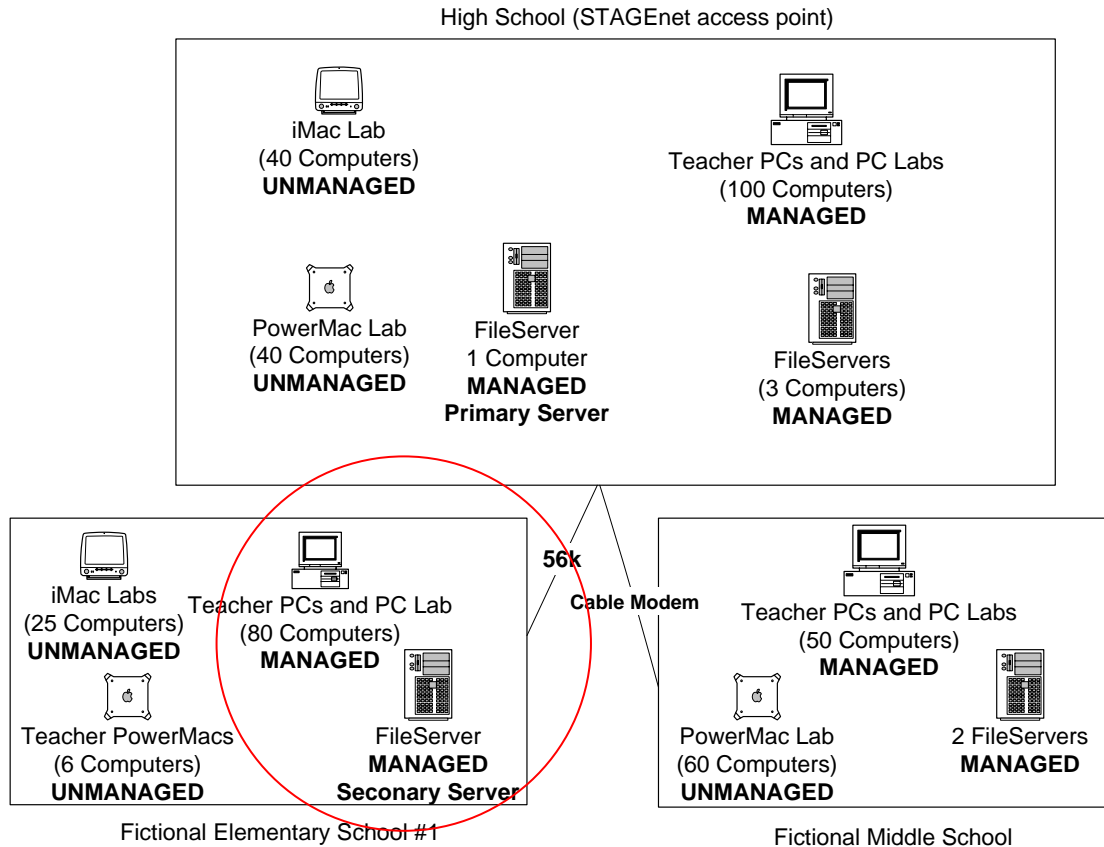


Figure 2 Since a large number of Managed computers would have to get updates via 56k, a secondary server was placed at that location.

Step 2: Preparing for Installation

Obtaining Media and Licenses (New Process)

You may install SAVCE as needed to ensure that your district's computers are protected. Once per year, EduTech will request information from you regarding the number of licenses in use and the operating systems of the computers where Symantec software is installed. This license allows installation of software on both desktops and file servers. Please note that every machine benefiting from virus protection **MUST** be licensed.

For example, if you have a file server with six machines attached, even if only the file server and four of the machines have SAVCE software on them, the other two machines must be licensed. Since they are accessing virus protected files, they are benefiting from the SAVCE software installed on the server.

Example:

Windows NT 4.0 Servers.....	2
Windows 2000 Server.....	1
Novell Server	1
Windows Desktops attached to the above servers .	105
Macintosh Desktops (no file server access).....	20
Windows Desktops (no file server access)	50
Total Lisc. Necessary	179

After you know how many licenses you will need, access the **North Dakota K-12 Symantec AntiVirus License Census** from www.edutech.nodak.edu/antivirus/census. If you find you need additional copies of the installation media, you may duplicate the CDs provided to you for district use or contact the EduTech Help Desk.

NOTE: EduTech has purchased these licenses for use in ND K-12 schools. Ownership and management of the license is not transferable to your school. So it is important to remember that all licenses are property of EduTech. This places certain restrictions on how you use the software. For instance:

- No participating school is entitled to an individual support contract with Symantec. All support questions must be directed to the EduTech Help Desk
- Software may not be installed on home computers. Formerly, Symantec allowed this practice, but now it is a ‘for-fee’ service which has not been purchased by EduTech. Also note from the bullet above that schools may not purchase this on their own, as they do not own the license.
- Every license purchased by EduTech will expire simultaneously in March 2008. License expiration dates are **not** determined by the date you request them.
- All licenses must be distributed with 2nd year maintenance. This is not optional, even for private schools. Without a current maintenance license you cannot legally receive virus definitions. Therefore for simplified administration, everyone will be on the same maintenance license cycle.

Periodically, EduTech may collect information from your district regarding the number and type of current SAVCE installations in your district.

Removing Current Antivirus Software

Before installing SAVCE software on any machine, you should uninstall any current antivirus software. Note that this includes previous versions of other Norton/Symantec AntiVirus products. Obviously you should attempt to minimize the amount of time your machines are in use without antivirus protection.

Step 3: Installing Symantec System Center and Snap-ins

Symantec System Center (SSC) is a module for the Microsoft Management Console. With this program you will interact with and manage your district's primary server. It is recommended that you install the SSC to your district's Primary Server first. However you may also install it on any other machines that you want to have control over the Primary Server.

1. Select a computer you will use to administrate your district's Primary Server (this can even be the Primary Server itself). This machine should be running Windows NT, 2000, XP or Server 2003 and have Internet Explorer 5.5 or later installed. Be certain that you have removed any previous versions of Norton/Symantec AntiVirus, Symantec System Center or other antivirus programs.

Note: If you are installing this software to a server with more than one network card, make sure the network interface that your clients will use to get definitions from is the first in the binding order.

- a. Click **Start**→**Settings**→**Control Panel**
 - b. Double-Click **Add/Remove Programs**
 - c. Select **Symantec System Center** and click **Remove**
 - d. Repeat steps **b** & **c** above for any of the following that appear in the applications list:
 - Norton/Symantec Antivirus Snap-in
 - Norton/Symantec Antivirus Add-On for Symantec System Center
 - Symantec Quarantine Console Snap-in Component
 - Symantec AntiVirus Server
 - e. (Optional) You may choose to delete the contents of the Temp folder and empty the Recycle Bin to free space on the server.
 - f. Restart the Server and log in as the local administrator.
2. Insert SAVCE CD Disc 1 (Windows Software) into the CD drive. If the "Symantec AntiVirus Corporate Edition" window does not appear automatically after a few moments, then locate SETUP.EXE on the CD drive's contents and double-click on it.
 3. After the setup interface appears, click **Install Administrator Tools** followed by **Install Symantec System Center**. Read the instructions on the Welcome screen and click **Next**.
 4. Read the license agreement carefully and click **I accept the terms in the license** and then click **Next**.
 5. Keep the defaults in the **Select Components** screen. Installation of AMS² is optional. Click **Next**
 6. You are now asked to choose the installation directory; it is recommended you accept the default selection and click **Next**.
 7. In the **Ready to Install the Program** screen, click **Install**.
 8. When the installation is complete, click **Finish** and then restart the computer

Step 4: Installing and Configuring Definitions Server Software

Installing Server Software

If you have not done so already, choose a single server to act as your district's Primary Server. Make sure you have installed the SSC described in the previous section to this server. After SSC has installed successfully, follow these instructions to set up the Symantec AntiVirus Server program. Only one server should need this installed. *The only exception would be if you identified places in your district that would benefit from Secondary AntiVirus Servers.*

1. Place SAVCE CD Disc 1 (Windows Software) in the CD tray of the Primary Server (make sure you are logged in with local administrator privileges). If the "Symantec AntiVirus Corporate Edition" window does not appear automatically after a few moments, then locate SETUP.EXE on the CD drive's contents and double-click on it.
2. Select the menu choice **Install Symantec AntiVirus → Deploy AntiVirus Server**.
3. At the Welcome screen, choose **Install** not Update and click **Next**.
4. Read the license agreement, select **I Agree** and click **Next**.
5. Install the Server Program. Installation of AMS² is optional.
6. In the Select Computers window you should see your computer's name in the left windowpane. Highlight that name and click on the **Add>** button.
7. Install to the default directory by clicking **Next**.
8. Primary Server Only: The software will ask you for a server group name. If you have already created a server group, select it from the list, if this is the first time you have created a server group, enter the name and click **Next**. If you created a new server group, click **Yes** when prompted to create the new group and enter username and password you wish to use for this server group.
9. Secondary Servers Only: The software will ask you for a server group name. You must select the group name you created for the Primary Server. Click **Next**.
10. Select **Automatic Startup** if it isn't already selected and click **Next**
11. Carefully read the information presented on the successive screens, clicking **Next** to continue to each one. When you click **Finish** the **Setup Progress** screen will display information regarding the install process.
12. You may get a warning that the definition files are out of date, ignore it for now and click **Close**.
13. If no errors are shown upon completion, click **Close** and reboot the server. If a server had listed errors, click the **View Errors...** button and contact the EduTech Help Desk with the information.

Auto-Protect will start on the computer as soon as Symantec AntiVirus is installed, but the Alert Management System² (AMS²) services will not start until after you restart the computer. If it is necessary to wait for a scheduled restart, the computer will be protected from the time of installation, but AMS² alerting will not work.

Note: Do not delete the NAV folder located by default at: <os drive>:\Program Files\NAV. A non-upgraded installation of Symantec AntiVirus server will create a folder called SAV located at \Program Files\SAV.

Making a Server the Primary Server

After the server has rebooted, you will need to configure the machine to be the Primary Server for the district.

1. Start up the Symantec System Center Console on the Primary Server
2. Expand the System Hierarchy to see your “Server Group”
3. Click once on System Hierarchy and then right click System Hierarchy and choose **View→Symantec Antivirus**.
4. Right click on your server group name and select **Unlock**. Enter the username and password for the server group (you created this in the previous section). The default password if it was not changed is ‘symantec’ without quotes.
5. Right click on your server’s name and select **Make Server a Primary Server**.
6. Read the notes in the dialog box. If making this computer the Primary Server, click **Yes**.

Configuring Your Definitions Source

Now you must configure the Primary Server to get its virus definition updates from Symantec Live Update. You would perform similar steps to inform your Secondary Server to get its definitions from your Primary Server.

1. Right click on your primary server and select: **All Tasks→ Symantec AntiVirus→Virus Definition Manager**
2. Next to **Update the Primary Server of the Server Group only** click **Configure**
3. In the window that pops up, click **Source**. Another window will appear.
4. Make sure **Live Update (Win32)/FTP (Netware)** is chosen. Click **OK**.
5. Click **Schedule** (which is below the **Source** button), click **Daily** for frequency and for time choose a time between 6:30 AM to 7:30 AM. While still in the **Virus Definition Update Schedule** window, click on **Advanced** and under **Randomization Options** uncheck **Perform update within plus or minus**. Click **OK**.
6. Click the **OK** on each open window until you return to the **Virus Definition Manager** window.
7. Under the **How Clients Retrieve Virus Definitions Updates** make sure **Update virus definitions from parent server** is check marked and **Schedule client for automatic updates using LiveUpdate** is un-checked. Click **OK**.
8. Click **OK** on each open window. You may now close SSC.

Allowing 10.0 Server to Manage 9.x Clients

The following steps **must** be performed to allow your SAVCE 10 server to manage older clients.

1. While still in the SSC, right mouse click on your Primary Server and select: **All Tasks**→**Symantec AntiVirus**→**Server Tuning Options**
2. Click first choice of **Allow this server to manage 9.x and earlier clients and servers (requires reboot to take effect)**. Click **OK**.

Backing up and restoring the pki folder

SAVCE 10 uses encryption to secure communication with SAVCE 10 clients. If the certificates used to validate the communication are lost (due to hardware failure or system migration) the relationship between the server and managed SAVCE 10 clients will be broken. Therefore we recommend backing up the folder on the server where these certificates are stored. This will minimize recovery time in the event of a primary server failure.

To back up the pki folder

The pki folder is located in the primary server's Symantec AntiVirus program folder. The default location depends on your operating system and whether you installed Symantec AntiVirus or Symantec Client Security:

- On a NetWare server, the default program folder is SYS:\SAV.
- When Symantec AntiVirus Corporate Edition server is installed on Windows, the default program folder is <OS drive>:\Program Files\SAV.
- When Symantec Client Security server is installed on Windows, the default program folder is <OS drive>:\Program Files\SAV\Symantec AntiVirus.

After you locate the pki folder, make a copy of it and secure it in a safe location such as a removable hard drive, thumb drive or burned onto a CD. This data should be kept in a vault or alternate location. In the event of a server failure and you have a backup copy of the pki folder (which also contains a needed registry value), you can restore communication by restoring both to their original locations on the primary server.

To restore communication on a Windows server

1. Reinstall the primary server using the same IP address and computer name.
2. Stop the Symantec AntiVirus service on the primary server.
3. Restore the pki folder to the Symantec AntiVirus Program folder.
4. Follow the directions in the "To set the DomainGUID value on a Windows server" section of this document.
5. Restart the Symantec AntiVirus service.

To set the DomainGUID value on a Windows computer

1. Start Windows Explorer.
2. Open the pki\private-keys folder.

3. Find the file that has this format:
 <computer name>.<key>.0.loginca.pvk
4. Write down or copy the <key> portion of the file name.
5. Start the Registry Editor.
6. Go to the HKEY_LOCAL_MACHINE\SOFTWARE\Intel\LANDesk\VirusProtect6\CurrentVersion key.
7. In the right pane, double-click **DomainGUID**.
8. Delete the data and replace it with the <key> text that you copied in step 4.
9. Go to the
 HKEY_LOCAL_MACHINE\SOFTWARE\Intel\LANDesk\VirusProtect6\CurrentVersion\DomainData key.
10. Repeat steps 7 and 8.
11. Exit the Registry Editor.

Step 5: Installing Windows Clients

Before installing any client software, remember to uninstall any anti-virus software that is currently installed. Also, if your district has Windows NT or 2000 servers, we would prefer that you set up your own Primary Server and not use the EduTech Primary server for your Managed clients. The EduTech Primary Server is provided for the benefit of schools that do not have servers on site.

Lastly, Windows XP users need to make a Local Security Policy change on their Windows XP systems. Under **Administrative Tools**, select **Local Security Policy**. In the left pane of the policy editor, navigate to Security **Settings/Local Policies/Security Options**. In the right pane, double-click **Network access: Sharing and security model for local accounts**. Change the setting to **Classic-Local users authenticate as themselves**.

1. At each machine[†], insert SAVCE CD Disc 1 (Windows Software). If the “Symantec AntiVirus Corporate Edition” window does not appear automatically after a few moments, then locate SETUP.EXE on the CD drive’s contents and double-click on it.
2. Choose **Install Symantec AntiVirus** → **Install Symantec AntiVirus** from the Install Menu.
3. At the Welcome screen, click **Next**. Read and accept the terms of the license agreement and click **Next**.
4. Choose **Client Install** if it is not already selected and click **Next**. Choose the **Complete** install and click **Next**.
5. The next screen presents you with two choices:
 - If you installed a Primary Server following the instructions above or if you want to let the EduTech Primary Server push definitions to your computer, select **Managed**.

[†] For information on performing alternate installation methods that do not require you to visit each machine, refer to Chapter 7 in the SAVCE Installation Guide (/Docs/savinst.pdf on Disc 1 of the SAVCE 10 media pack)

Note: If your district has Windows servers, we would prefer that you set up your own Primary Server and not use the EduTech Primary server for your Managed clients. The EduTech Primary Server is provided for the benefit of schools that do not have servers on-site.

- If you did not install a Primary server per the instructions above and you do not want to use the EduTech Primary server then select **Unmanaged**. Computers that are configured in this way will use LiveUpdate to get their virus definitions from Symantec's servers at scheduled intervals.
- 6. If you selected **Managed**, the next screen asks for the server name. Enter the IP address of your Primary Server (preferably) or the address of the EduTech Primary Server by clicking **Browse → Find Computer** and in **Search For** type doctor.sendit.nodak.edu after which click **Find**. Finish by clicking **OK** and **Next**.
- 7. The installation program will generate the install script. When it is complete, click **Install**.
- 8. After the client install is completed, click **Finish**. You may see a warning that the virus definitions are out of date. Within about an hour the SAVCE 10.0 client will update itself from the Primary server you selected during the install. If it does not, contact the EduTech Help Desk.
- 9. If you selected **Unmanaged** then just finish the installation. The end of the install will ask you to run LiveUpdate, keep this choice checked to update the Virus Definitions for the unmanaged client immediately.

Step 6: Installing Macintosh Clients

The server software cannot currently manage Macintosh computers so you will need to install the client for Macintosh computers and then setup the LiveUpdate schedule to get virus definitions and program updates from Symantec's site.

1. Insert Disc 2 of the SAVCE media in the Macintosh.
2. When the CD contents are displayed on screen, open the appropriate install folder.
 - a. **Norton AntiVirus 10.0** is required for OS 10.4 or OS 10.3. To install this version, open the folder and double-click on **Norton AntiVirus Installer.mpkg**. Follow the instructions presented onscreen to complete the install.
 - b. The **Norton AntiVirus 9.0** folder contains both Norton AntiVirus 9.0 and Norton AntiVirus 7.0.2. Version 9.0 is required for OS 10.1.5 or OS 10.2 while version 7.0.2 is designed for OS 9 and earlier.
 - i. In **Install for OS 9**, double-click **Install Norton AntiVirus**.
 - ii. In **Install for OS X**, double-click on **Norton AntiVirus Installer**.
3. Continue with the install until it is finished then reboot the Macintosh as the program recommends.