Good Samaritan Health and Wellness Center
Policies and Procedures

Subject: Computer Virus Protection	Policy #: 4.9.8
Prepared by: John Hilliard	Revision #:
Approved by: Board of Directors	Effective Date: 06/16/16

4.9.8 Computer Virus Protection

PURPOSE:

It is the responsibility of all users of Good Samaritan Health and Wellness computer network to take reasonable measure to protect the network from computer virus infections. This policy outlines how various viruses can infect eh network, how the I.T. department works to prevent and /or minimize infections, and how network users should respond to virus if it is suspected to have infected a computer or Network.

SCOPE:

This policy relates to any Good Samaritan Health and Wellness computer, laptop, server or other device attached to the WAN or the Internet. Compliance to this policy applies to any user of Good Samaritan Health and Wellness computer services.

BACKGROUND:

True viruses actually hide themselves, often as macros, within other files, such as spreadsheets or word processing documents. When an infected file is opened from a computer connected to the Good Samaritan Health and Wellness network, the virus can spread throughout the network and may do damage.

Viruses can enter the network in a variety of ways:

- E-mail—Most viruses are sent as e-mail attachments. These attachments could be working documents or spreadsheets, or they could be merely viruses disguised as pictures, jokes, etc. However, once some viruses are opened, they automatically e-mail themselves, and the sender may not know his or her computer is infected.

- Disk, CD, Zip disk, Flash/Thumb drives, or other media—Viruses can also spread via various types of storage media. As with e-mail attachments, the virus could hide within a legitimate document or spreadsheet or simply be disguised as another type of file.
- Software downloaded from the Internet—Downloading software, music or video via the Internet can also be a source of infection. As with other types of transmissions, the virus could hide within a legitimate document, spreadsheet, or other type of file.

Good Samaritan Health and Wellness's I.T. department fights viruses in several ways:

True viruses actually hide themselves, often as macros, within other files, such as spreadsheets or word processing documents. When an infected file is opened from a computer connected to the Good Samaritan Health and Wellness network, the virus can spread throughout the network and may do damage.

Viruses can enter the network in a variety of ways:

- E-mail—Most viruses are sent as e-mail attachments. These attachments could be working documents or spreadsheets, or they could be merely viruses disguised as pictures, jokes, etc. However, once some viruses are opened, they automatically e-mail themselves, and the sender may not know his or her computer is infected.
- Disk, CD, Zip disk, Flash/Thumb drives, or other media—Viruses can also spread via various types of storage media. As with e-mail attachments, the virus could hide within a legitimate document or spreadsheet or simply be disguised as another type of file.
- Software downloaded from the Internet—Downloading software, music or video via the Internet can also be a source of infection. As with other types of transmissions, the virus could hide within a legitimate document, spreadsheet, or other type of file.

Good Samaritan Health and Wellness's I.T. department fights viruses in several ways:

Scanning Internet traffic—All Internet traffic coming to and going from our network must pass through company servers and other network devices.

Routinely updating virus definitions—When end users turn on their computers, the workstation virus protection program checks with a Good Samaritan Health and Wellness server on the network for updates. The workstation program will then download and install the update automatically, if one exists.

The Good Samaritan Health and Wellness I.T. department has also implemented policy to ensure that all computers and servers maintained up-to-date, patched applications.

Policy:

To conduct the business of Good Samaritan Health and Wellness requires that computer systems and networks be operated in a safe and secure manner. The primary responsibility for this requirement is assigned to the "Security Officer" and the I.T. staff. However, every staff

member is charged with the responsibility to use the provided services for the purposes intended and to comply with all security requirements.

Anti-Virus

All Good Samaritan Health and Wellness personal computers and servers must employ a computer virus protection program. All network-attached PCs shall have the Avast Anti-Virus application installed and receive timely virus definition updates from the Avast Anti-Virus server.

Software Patches

All Microsoft-based operating systems will be updated with the latest security patches. Review of current system patch levels and deployment of corrective patches will be performed by the I.T. Department through the Microsoft Server Update Service (WSUS). Priority will be given to critical patches.

Software Downloading from Internet

Downloading software, music or video via the Internet is prohibited unless prior approval is obtained from a member of the I.T. Department or the Security Officer

External Storage Devices

Due to the high level of vulnerability Good Samaritan Health and Wellness Center prohibits access and use of external storage devices (external hard drives, flash drives, CDs, DVDs,) without prior approval of a member of the I.T department or security officer.

1. VIOLATION REPORTING

If you receive a suspicious file or e-mail attachment, do not open it.

Any observed misuse or violation of this policy should be immediately reported to one of the following persons:

- Executive Director,
- Chief Financial Officer,
- Security Officer