Good Samaritan Health & Wellness Center, Inc.

Policies and Procedures

Subject: Remote Network Access	Policy # 4.9.13
Prepared by Ray Bowyer	Draft 4/8/16
Approved by: Board of Directors	Effective Date: 7/21/2016

4.9.13 Remote Network Access

PURPOSE

This policy provides the guidelines for granting, configuring and revoking of remote network access privileges, including dial-up and virtual private network (VPN) access, for Good Samaritan Health and Wellness Center.

SCOPE

This policy applies to any person or entity granted access to the Good Samaritan Health and Wellness Center network from external locations. These users are divided into three separate groups:

- Administrators – These are logins used for configuration and control of the equipment.
- Vendors/Partners – These accounts are used by supporting vendors to supplement or augment Good Samaritan Health and Wellness Center resources.
- Staff/volunteers – Staff/volunteer accounts allows remote access to Good Samaritan Health and Wellness Center resources/services.

POLICY

- Remote network access privileges require approval of the Information Security Officer (currently Rhonda Hunt).
- Remote network access privileges to third-party vendors require a determination by the IT team that these vendors have a legitimate business need for such access, these privileges will only be enabled for the time period required to accomplish approved tasks. Additionally, the vendor must be operating under contract or MOU (memorandum of understanding) with Good Samaritan Health and Wellness Center and have completed a Business Associate Agreement (BAA).
- Remote network access connections must be configured according to approved guidelines and standards.

- Good Samaritan Health and Wellness Center reserves the right to revoke remote network access without notice. A staff member's authority to access is immediately severed at termination.
- The list of approved Remote Network Access users will be reviewed annually during the annual Risk Assessment per Policy 4.9.15 and may require the user to re-submit paperwork to justify continued access. The annual Risk Assessment will be reviewed by the CEO.
- In most cases, the remote access will allow access to the staff member's assigned work computer. This procedure would have all information stored only on the organization's owned equipment. In no case should PHI or security information be saved or stored on a staff member's home or personal computer without appropriate safeguards.
- Staff must always be aware of their surroundings when performing remote network access. Make sure that all confidential information is not viewable by others.
- At no time should you allow your remote network connection to be used by others.
- At no time should you share, record, disclose or store access passwords where they can become available to others.
- Do not save passwords for the remote access or work computer logins.
- If you believe your home or personal computer has been infected with virus or spyware applications – do not access the Good Samaritan Health and Wellness Center network.

Violation of this policy will lead to the immediate suspension of remote access rights and may require the user to complete a security awareness training class prior to access rights being re-established.

PROCEDURE

To Request Remote Access Authorization:

1. Staff or partners must write a letter to the Security Officer stating the reason access is needed, and for what period of time.
2. After approval by the Security Officer, access rights will be assigned by the IT team to the staff member or partner.
3. The IT team will provide remote access for the time approved.

VIOLATION REPORTING

Any observed or suspected violation of this policy should be immediately reported to the Security.

DEFINITIONS

Personal Health Information (PHI) – Individually identifiable health information that is:

- Transmitted by electronic media;
- Maintained in electronic media; or
- Transmitted or maintained in any other form or medium.

Virtual Private Network (VPN) – A secure connection to a private network created on the public telecommunication infrastructure or Internet.