# Cornerstone Behavioral Healthcare

## Remote Access Policy

### 1. Overview

This policy is to inform all employees of Cornerstone Behavioral Healthcare that we have and use many different connections around the company's network from LogMeIn Hamachi to having the ability to work from home, or for outside venders such as PIMSY to troubleshoot software from outside of the domain. We are also using VPN software internally to remotely connect for troubleshooting and to see and configure computers around the company's internal domain to keep them current for function as well as protection. This general policy covering Cornerstone's best interests regarding use and maintaining security measures is important.

### 2. Purpose

The purpose of this policy is to define standards for connecting to Cornerstone's network from any host. These standards are designed to minimize the potential exposure to Cornerstone from damages which may result from unauthorized use of Cornerstone's resources. Damages include the loss of company sensitive and/or confidential data, theft of intellectual property, a diminished public image, an attack on critical Cornerstone internal systems, and other potential negative outcomes.

### 3. Scope

This policy applies to all Cornerstone employees, contractors, vendors and agents with a Cornerstone - owned or personally-owned computer or workstation used to connect to the Cornerstone network. This policy applies to remote access connections used to do work on behalf of Cornerstone including reading or sending email and viewing intranet web resources. Remote access implementations that are covered by this policy include, but are not limited to RDC, VPN, SSH.

### 4. Policy

It is the responsibility of Cornerstone employees, contractors, vendors and agents with remote access privileges to Cornerstone's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to Cornerstone.

For additional information regarding Cornerstone's remote access connection options, including how to connect, please contact the IT-Helpdesk. Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong pass-phrases. At no time should any Cornerstone employee provide their login or email their password to anyone -- not even family members, other than IT Administrators. Cornerstone employees and contractors with remote access privileges must ensure that their Cornerstone-owned or personal computer or workstation, which is remotely connected to Cornerstone's network, is not simultaneously connected to any other network, with the exception of personal networks that are under the complete control of the user.
Cornerstone employees and contractors with remote access privileges to Cornerstone's corporate network must not use non-Cornerstone email accounts (e.g., Hotmail, Yahoo, AOL), or other external resources to conduct Cornerstone business, thereby ensuring that official business is never confused with personal business. Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time. Non-standard hardware configurations and security configurations for access

to hardware must be approved by Cornerstone. All hosts that are connected to Cornerstone internal networks via remote access technologies must use the most up-to-date anti-virus software (Microsoft security essentials), and this includes personal computers. Third party connections must comply with requirements. Personal equipment that is used to connect to Cornerstone's networks must meet the requirements of Cornerstone-owned equipment for remote access. Organizations or individuals who wish to implement non-standard Remote Access solutions to the Cornerstone production network must obtain prior approval from Cornerstone. As a courtesy to Cornerstone employees, we will give proper effort to call said remote destination before taking over and installing updates remotely.

Remote watching of a system will only be used as a measure to confirm suspicions of improper use of company computers or as a second way to watch camera systems within the company areas for designated employees for security purposes.

### 5. Policy Compliance

Regarding compliance measurement, the Cornerstone team will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner. Any exception to the policy must be approved by the Cornerstone Leadership Team in advance. Non-compliance of an employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Donna M. Ruble, LCPC
Executive Director/Date

Reviewed and revised 04-29-15 LT