GREATER COLUMBIA BEHAVIORAL HEALTH, LLC. BH-ASO

Remote Access Procedure

No: PS609

Document Type:[1] X Policy & Procedure ___ Process Guideline ___ Plan ___ System Description

Adopted: 1/1/2019
Last Reviewed: ~~1/25/2021~~4/10/2024
Retired:

Revisions: 2/28/2020

Document Scope: (applies to Policy & Procedure only)

– The requirements herein apply only to the GCBH BH-ASO Central Office and its functions.

X The requirements herein apply, verbatim, to GCBH BH-ASO and its network providers[2].

– The requirements herein apply ~~both to GCBH BH-ASO and its~~to both GCBH BH-ASO and its network providers[2]. Additionally, network providers must have internal documents outlining their processes for implementing the requirements, insofar as they relate to actions for which network providers are responsible.

Formatted: Highlight

Formatted: Underline

PURPOSE: To establish procedures to optimize the efficiency of Greater Columbia Behavioral Health (GCBH BH-ASO) remote access program.

DEFINITIONS

I. Remote access: A generic term used to describe the accessing of the computer network by individuals not located at the organization's primary office. This may take the form of traveling employees, employees who regularly work from home, or employees who work both from the office and from home.

POLICY

A. Both GCBH BH-ASO and the employee may benefit from the increased flexibility provided by a remote access program.

B. Participation in a remote access program may not be possible for every employee. Remote access is meant to be an alternative method of meeting GCBH BH-ASO needs. The Agency may refuse to extend remote access privileges to any employee or terminate a remote access arrangement at any time.

PROCEDURE

1. Acceptable Use:

   1.1. Hardware devices, software programs, and network systems purchased and provided by GCBH BH-ASO for remote access are used only for creating, researching, and processing Agency-related materials. By using GCBH BH-ASO hardware, software and network systems, employees assume personal responsibility for their appropriate use and agree to comply with this policy and other applicable policies, as well as City, State and Federal laws and regulations.

2. Equipment & Tools:

   2.1. GCBH BH-ASO provides tools and equipment for remotely accessing the corporate network system in a secure manner. This includes computer hardware, software, ~~phone lines,~~ e-mail, voicemail, VPN hardware and software, connectivity to host applications, and other applicable equipment as deemed necessary.

[1]See definitions of document types in AD100, "Development, Approval & Review of Formal GCBH BH-ASO Documents"
[2]"Network Provider" – An organization with which GCBH BH-ASO is contracted for the provision of direct services.

2.2. The use of equipment and software for remotely accessing the computer network is limited to authorized persons and for purposes relating to GCBH BH-ASO business. GCBH BH-ASO provides for repairs to their equipment. When the employee uses their own equipment, the employee is responsible for maintenance and repair of their equipment.

3. Password and Privacy Protection:

3.1. When using GCBH BH-ASO hardware, software and network systems employees assume personal responsibility for their appropriate use and agree to comply with GCBH BH-ASO Password Protection policy. In addition, the employee agrees to take maximum precautions to prevent unauthorized access and/or viewing of individual's protected health information during remote access sessions. To do this, employees agree to place the computer in a secure environment (not in open living rooms or other common spaces) and to log-off of the GCBH BH-ASO network when absent from the computer.

4. Use of Personal Computers and Equipment:

4.1. Information Services department will only provide support for equipment and software provided by GCBH BH-ASO.

4.2. The employee's personal computer must have a valid anti-virus software application on their system. The employee agrees to install and maintain this software along with any virus definition updates that are issued. The employee will need to bring their system into the GCBH BH-ASO office, where IS staff will verify the anti-virus application and then install the VPN client.

4.3. Multi-factor authentication (MFA) is required for connecting to the GCBH BH-ASO network. For the Convenience of the staff and for GCBH, a MFA app may be installed on the employee's personal phone or they may choose to receive text messages to their personal phone instead rather than being assigned a MFA key fob device.

~~4.3.~~4.4. The employee agrees to install and maintain any and all software patches issued by the Information Services department. GCBH BH-ASO will bear no responsibility if the installation or use of any necessary software causes system lockups, crashes, or complete or partial data loss. The employee is solely responsible for backing up data on their personal machine before beginning any work. At its discretion, GCBH BH-ASO will disallow remote access for any employee using a personal home computer that proves incapable, *for any reason*, of not working correctly with GCBH BH-ASO-provided software, or being used in a production environment. If the employee has a critical need for remote access and the employee's personal computer(s) is unsuitable for the task, the employee should submit a formal request for GCBH BH-ASO equipment to be provided. This request should flow through the employee's Manager to the Information Services Manager.

Formatted: Font: Not Italic, No underline

~~4.4.~~4.5. Employees are strictly prohibited from downloading, copying, or otherwise keeping individual's protected health information on personal computers.

5. Enforcement:

5.1. Any employee who violates the Remote Access Procedure will be subject to discipline up to and including termination from employment in accordance with GCBH BH-ASO's Sanction Policy.

APPROVAL

Karen Richardson or Sindi Saunders, Co-Directors	Date