Document Type:[1]	___ Policy & Procedure	_X_ Process Guideline	Adopted:	1/1/2019
			Last Reviewed:	2/28/2020
	___ Plan	___ System Description	Retired:	

Revisions: 2/28/2020

Document Scope: (applies to Policy & Procedure only)

X – The requirements herein apply only to the GCBH Central Office and its functions.

– The requirements herein apply, verbatim, to GCBH and its network providers[2].

– The requirements herein apply both to GCBH 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.

PURPOSE: To define the procedure and responsibility for all staff of Greater Columbia Behavioral Health (GCBH) who use computer desktop, laptop, or mobile device.

PROCEDURE

1. **Workstation Use**:

1.1. Personnel using GCBH computer desktops, laptops with docking stations, IP phone sets, or any other GCBH electronic device needs to secure a safe area for their drinks and food to prevent damage due to spills and so forth to GCBH electronic equipment.

1.2. Personnel logging onto the system should use care when logging into the GCBH network to ensure that no one observes the entry of their password.

1.3. Personnel shall neither log onto the system using another staff's password nor permit another staff member to log on with their password. GCBH personnel shall not enter data under another staff member's password. Please refer to the Password Protection Procedure.

1.4. After three failed attempts to log on, the system holds the account disabled for 30 minutes. The GCBH staff member can then retry their password or contact the GCBH System Administrator.

1.5. GCBH personnel using GCBH computer equipment/network access are responsible for the content of any data he/she inputs into the computer or transmits through or outside the GCBH network system. No GCBH staff personnel may hide their identity as the author of the entry or represent that someone else entered the data or sent the message. All GCBH personnel familiarize themselves with and comply with GCBH e-mail policy.

1.6. GCBH personnel are only authorized to access information based on their Title or Role at GCBH. No employee shall disclose confidential or other information unless properly authorized (GCBH Confidentiality Policy and the Disclosure Policy).

1.7. Personnel will not leave printers unattended when they are printing confidential information. This rule is especially important when two or more

[1]See definitions of document types in AD100, "Development, Approval & Review of Formal GCBH Documents"

[2]"Network Provider" – An organization with which GCBH is contracted for the provision of direct services.

computers share a common printer or when the printer is in an area where unauthorized personnel have access to the printer.

1.8. Personnel shall not use the GCBH network or related computer equipment to solicit for outside business ventures, organizational campaigns, or political or religious causes. They shall not enter, transmit, or maintain communications of a discriminatory or harassing nature or materials that are obscene or x-rated. No person shall enter, transmit, or maintain messages with derogatory or inflammatory remarks about an individual's race, age, disability, religion, national origin, physical attributes, sexual preference, or health condition. No person shall enter, maintain, or transmit any abusive, profane, or offensive language.

1.9. Personnel using the GCBH network or computer equipment will not write down their password and place it at or near the computer/laptop, such as putting their password on a yellow "sticky" note on the screen or on a piece of tape under the keyboard.

1.10. Each computer desktop/laptop is programmed to generate a password protected screen saver that actives after 15 minutes of idle time.

1.11. Users log off the system if he/she leaves the computer desktop/laptop for more than 20 minutes or if he/she is leaving the premises.

1.12. No personnel shall downloads protected health information (PHI) from GCBH network onto USB, CD, hard drive, fax, scanner, any network drive or any other hardware, software, or paper without the express permission of their manager with written notice to the IS Manager, who in turn notifies the HIPAA Officer.

1.13. No personnel shall download any software without express written permission of the IS Manager. The IS Manager must approve any software that an employee wishes to download in order to protect against the transmission of computer viruses into the system.

2. Laptop Computer:

2.1. Officers, agents, employees, contractors, and others using laptop computers (users) must read, understand, and comply with this policy.

2.2. No user shall, for any purpose, download, maintain, or transmit confidential or other PHI on a computer without the written authorization of the HIPAA Officer upon the recommendation of their manager.

2.3. Any portable equipment requested is logged in the Information Services equipment log. The hardware, software, all related components, and data are the property of GCBH and must be safeguarded and returned upon request and upon termination of employment. All staff are responsible for any equipment GCBH issues to them during their employment.

2.4. The user agrees to use the equipment solely for GCBH business purposes and further understands:

2.4.1. VPN functions are restricted to connecting to the GCBH network. The user is not permitted to connect into any other unauthorized services, Internet service providers, or any other Internet access or to use the VPN capabilities in any other manner than as instructed. The user understands that the hardware has been disabled from performing any functions other than those intended for business use and that the user may not attempt to enable such other functions.

2.4.2. Computers, associated equipment, and software are for business use only, not for the personal use of the user or any other person or entity.

2.4.3. Users will not download any software onto the computer except as loaded by authorized staff of the Information Services department.

2.4.4. Users will not insert any USB devices, CDs, or other media into the computer without the express authorization of the Information Services Manager except GCBH formatted devices used to create backups of user data.

2.4.5. Users must use only batteries and power cables provided by GCBH and may not, for example, use their car's adaptor power sources.

2.4.6. Users will not connect any non-GCBH peripherals (keyboards, printers, modems, etc.) without the express authorization of the Information Services department.

2.4.7. Users are responsible for securing the unit, all associated equipment, and all data, within their homes, cars, and other locations as instructed in the training provided.

2.4.8. Users may not leave laptop computer units unattended unless they are in a secured location.

2.4.9. Users should not leave laptop computer units in cars or car trunks for an extended period in extreme weather (heat or cold) or leave them exposed to direct sunlight.

2.4.10. Users must place laptop computers and associated equipment in their proper carrying cases when transporting them.

2.4.11. Users must not alter the serial numbers and asset numbers of the equipment in any way.

2.4.12. Users will not permit anyone else to use the computer for any purpose, including, but not limited to, the user's family and/or associates, individuals, individual's families, or unauthorized officers, employees, and agents of GCBH.

2.4.13. Users must not share their passwords with any other person and must safeguard their passwords against unauthorized use. (See the Password Protection procedure).

2.4.14. Users must report in writing any breach of password security immediately to the IS Manager.

2.4.15. Users must maintain confidentiality when using the computers. The screen must be protected from viewing by unauthorized personnel, and users must properly log off the laptop when it is not in use.

2.4.16. Users must immediately report in writing any lost, damaged, malfunctioning, or stolen equipment or any breach of security or confidentiality to the IS Manager.

3. Enforcement:

3.1. All managers are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination from employment in accordance with GCBH's Sanction Policy

APPROVAL

Karen Richardson

Karen Richardson or Sindi Saunders, Co-Directors

2/28/2020

Date