

Document Type: ¹	☐ Policy & Procedure	☒ Process Guideline	Adopted: 1/1/2019
	☐ Plan	☐ System Description	Last Reviewed: 3/11/2026
			Retired: _____

Revisions: 2/28/2020, 1/24/2022, 4/14/2022, 7/8/2024, 3/11/2026

Document Scope: (applies to Policy & Procedure only)

- ☒ The requirements herein apply only to the GCBH BH-ASO Central Office and its functions.
- The requirements herein apply, verbatim, to GCBH BH-ASO and its network providers².
- The requirements herein apply to both GCBH BH-ASO and its network providers². 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 BH-ASO) who use computer desktop, laptop, or mobile device.

POLICY

- A. Officers, agents, employees, contractors, and others using laptop computers (users) must read, understand, and comply with this policy.
- B. Personnel shall safeguard their passwords from unauthorized access or misuse.
- C. GCBH BH-ASO personnel are only authorized to access information based on their Title or Role at GCBH BH-ASO. No employee shall disclose confidential or other information unless properly authorized (GCBH BH-ASO Confidentiality Policy and the Disclosure Policy).
- D. The user agrees to use the equipment solely for GCBH BH-ASO business purposes. Personnel shall not use the GCBH BH-ASO 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. Due to GCBH BH-ASO being funded by public funds, all electronic communication, files, and data may be subject to public records requests; staff should consider all work that is done on GCBH equipment and during GCBH time as available for public consumption.
- E. Computers, associated equipment, and software are for business use only, not for the personal use of the user or any other person or entity. Users will also not permit anyone else to use the computer for any purpose, including, but not limited to, the user's family and/or associates, or unauthorized officers, employees, and agents of GCBH BH-ASO.

PROCEDURE

1. Workstation and Portable Device Use:

- 1.1. Personnel using GCBH BH-ASO computer desktops, laptops, phones, or any other GCBH BH-ASO electronic device needs to secure a safe area for their drinks and food to prevent damage due to spills and so forth to GCBH BH-ASO electronic equipment.
- 1.2. Personnel logging onto the system should use care when logging into the GCBH BH-ASO 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 BH-ASO 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 BH-ASO staff member can then retry their password or contact the GCBH BH-ASO IS Department to manually unlock their account.
- 1.5. GCBH BH-ASO personnel using GCBH BH-ASO computer equipment/network access are responsible for the content of any data they input into the computer or transmit through or outside the GCBH BH-ASO network system. No GCBH BH-ASO 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 BH-ASO personnel familiarize themselves with and comply with GCBH BH-ASO e-mail policy.
- 1.6. Personnel will not leave printers unattended when they are printing confidential information. This rule is especially important when two or more computers share a common printer or when the printer is in an area where unauthorized personnel have access to the printer.
- 1.7. Personnel using the GCBH BH-ASO 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 "sticky" note on the screen or on a piece of tape under the keyboard.
- 1.8. Each computer desktop/laptop is programmed to generate a password protected screen saver that activates after 15 minutes of idle time.
- 1.9. Users log off the system if they leave the computer desktop/laptop for more than 20 minutes or if they are leaving the premises.
- 1.10. No personnel shall download, maintain, or transmit confidential or other protected health information (PHI) from GCBH BH-ASO 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.

- 1.11. 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.
- 1.12. 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 BH-ASO and must be safeguarded and returned upon request and upon termination of employment. All staff are responsible for any equipment GCBH BH-ASO issues to them during their employment.
- 1.13. VPN functions are restricted to connecting to the GCBH BH-ASO 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.
- 1.14. Users will not insert any USB devices, CDs, or other removable media into the computer without the express authorization of the Information Services Manager except GCBH BH-ASO formatted devices used to create backups of user data.
- 1.15. Users must use only batteries and power cables provided by GCBH BH-ASO and may not, for example, use their car's adapter power sources.
- 1.16. Users will not connect any non-GCBH BH-ASO peripherals (keyboards, printers, modems, cameras, etc.) without the express authorization of the Information Services department.
- 1.17. 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.
- 1.18. Users may not leave laptop computer units unattended unless they are in a secured location.
- 1.19. 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.
- 1.20. Users must place laptop computers and associated equipment in their proper carrying cases when transporting them.
- 1.21. Users must not alter the serial numbers and asset numbers of the equipment in any way.
- 1.22. Users must report in writing any breach of password security immediately to the IS Manager.

- 1.23. 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.
- 1.24. Users must immediately report in writing any lost, damaged, malfunctioning, or stolen equipment or any breach of security or confidentiality to the IS Manager.
- 1.25. Since GCBH BH-ASO uses Duo for multi-factor authentication, if a user is gifting or surplussing a mobile phone with the GCBH BH-ASO connection info on it, the user must delete the connection from their Duo app and do a factory reset on the phone to clear it. If the mobile device has been lost or stolen or is otherwise unable to remove that connection from their Duo app, the user must notify the IS Department immediately so the device can be removed as authorized from the Duo management portal.

2. Enforcement:

- 2.1. 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 BH-ASO's Sanction Policy.

APPROVAL



Karen Richardson or Sindi Saunders, Co-Directors



Date