Document Type:[1]	X Policy & Procedure	___ Process Guideline	Adopted:	1/1/2019
			Last Reviewed:	11/1/2022
	___ Plan	___ System Description	Retired:	

Revisions: 2/28/2020, 1/22/2021, 11/1/2022

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 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 address security related items to ensure the integrity of data and the privacy of our individual data from unauthorized access.

DEFINITIONS

I. None

POLICY

A. Security Overview. The GCBH BH-ASO regional office is responsible for establishing and maintaining processes and procedures that are aligned with industry best practices to ensure the security and integrity of the technology resources use to create, access, and/or store confidential data. This policy addresses:

- Storage location of user generated data files
- Backup and testing of data
- Workstation resiliency (restoration / substitution)
- Anti-virus / anti-spam
- Authorized access (password requirements, lockout, screensaver, password history)
- Portable Systems / Media
- Business Continuity / Disaster Recovery Requirements
- Data Security for surplus items
- Server Room Security
- Internet Security
- Wireless Security

[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.

PROCEDURE

Minimum Requirements:

1. Ensure that the event viewer and security logs are activated on all computer servers, and desktop computers where applicable.
2. Ensure that all computer servers are backed up at least weekly. An effort is to be made to keep data files as centralized as possible on appropriately designated GCBH BH-ASO Servers.
    2.1. Differential backups are done between a full data dump.
    2.2. Backup tapes are tested at least annually.
        2.2.1. Testing is done by the alternate backup operator opposed to the lead backup operator when possible.
        2.2.2. Testing is completed through the use of restoring a file from one of the backup sets.
3. GCBH BH-ASO's method to ensure quick restore of the desktop/laptop environment is through the use of spare desktop/laptop systems. Also, remote management agents installed on desktop/laptop computers is utilized for technical support to the end user base.
4. Virus and malware protection is installed, kept up-to-date, and running on all computers and servers including the e-mail server.
5. Every effort is made to prevent unauthorized access of data. All desktop computers are password protected, and screen savers activated. In addition, computer monitors and printers are located as to eliminate unauthorized viewing.
    5.1. Minimum standards are:
        5.1.1. Password setting is eight alphanumeric character minimum, from at least three of the following;
        5.1.2. Upper case.
        5.1.3. Lower case.
        5.1.4. Numbers/special characters.
    5.2. Lockout occurs after three bad attempts (for thirty-minute duration, or administrator intervention);
    5.3. The password is changed by each user at least every sixty days;
    5.4. There is a Domain GPO for password history that prohibits the use of 5 prior passwords.
    5.5. Screensavers are activated and password protected (after 15 minutes);
    5.6. Passwords are not posted on or near workstation.
6. Floppy disks, memory keys, and other removable media and hardware are not to be left out unsecured, and any PHI on these devices is encrypted or password protected.
7. A Disaster Recovery Plan (HIPAA and BBA compliant) is in place.

8. Portable systems (i.e., laptops, iPads, tablets, smart phones) are stored securely.
9. Computers, laptops, memory keys/removable media, and servers are cleaned of Protected Health Information (PHI) before reassignment or surplus.
10. The server room is kept as secure as possible.
    - 10.1. The door is closed and locked with minimal key distribution to authorized personnel.
    - 10.2. Unused keys are secured.
    - 10.3. Air temperature is maintained as per server requirements.
    - 10.4. Network devices (i.e., hub, wireless access, router, etc.) are located in server room or secured area.
    - 10.5. There is an uninterrupted power supply UPS in use for all user computers.
    - 10.6. Fire extinguishers are checked and rated for electrical fires dedicated to server room.
    - 10.7. Log files on servers and desktop computers are NOT saved to a logging system for future review. Old data will be overwritten as the computer logs fill.
    - 10.8. In the event that maintenance or repairs need to be completed in the server room by outside vendors, they will be monitored and their access will be limited to prevent unauthorized access or risk to PHI.
11. A Firewall is used to protect all internet access.
12. The GCBH BH-ASO IS Manager holds sole responsibility for accessing any software or application for the purposes of their being revised, tested, or updated.

APPROVAL

Karen Richardson or Sindi Saunders, Co-Directors — Date: 11/1/2022