
Document Type: ¹	<input checked="" type="checkbox"/> Policy & Procedure	<input type="checkbox"/> Process Guideline	Adopted:	1/1/2019
	<input type="checkbox"/> Plan	<input type="checkbox"/> System Description	Last Reviewed:	7/8/2024
			Retired:	

Revisions: 1/27/2021, 7/8/2024

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 areas and the procedures for protecting Greater Columbia Behavioral Health (GCBH BH-ASO) equipment and networks from the potent threat of software virus intrusion and infection.

POLICY

- A. This policy is specifically designed to address GCBH BH-ASO protection against viruses and malware.
- B. Violation of this policy may subject employees or contractors to disciplinary procedures up to and including termination.
- C. Questions about this policy may be directed to the IS Manager.

PROCEDURE

- 1. Workstations and Laptops:
 - 1.1. GCBH BH-ASO Recommended Primary Controls at Desktop Anti-Virus Level. These controls will be implemented by the Information Services department unless otherwise indicated:
 - 1.1.1. Install certified anti-virus software on all workstations and laptop PCs and workstations;
 - 1.1.2. Subscribe to the alert service and virus definition file update service provided by the software vendor. Continuous monitoring of the software vendor's site for updates will be the responsibility of a designated Information Services Department staff;
 - 1.1.3. Workstation and laptop anti-virus software (virus signatures) will be updated automatically through the online anti-virus console. No user intervention will be required;
 - 1.1.4. Perform emergency updates within one business day after an alert;
 - 1.1.5. Implement the following workstation/laptop/server anti-virus software configuration:
 - 1.1.5.1. Enable full-time, background, real time, auto-protect or similar mode;
 - 1.1.5.2. Enable start-up scanning of memory, master / boot records, system files;

- 1.1.5.3. Configure scanning/checking options to include checking for all files; and
- 1.1.5.4. Enable logs for all desktop virus-related activity.
- 1.1.6. Subscribe to alert services from office productivity suite vendors and install all recommended security updates automatically through the use of network software policies and perform monthly network maintenance.
- 1.2. Additional notes on workstation and laptop level policies:
 - 1.2.1. Alerts to users are neither recommended nor discouraged. However, system administrator alerts, logs, or other advisories are continuously enabled. User controls over the anti-virus software are set to prevent users from “canceling” a virus alert.
 - 1.2.2. User-driven scanning policies such as requesting users to scan media, downloads, or hard drives are not recommended as they are generally more expensive and infringing than useful.
- 2. E-Mail Gateways, Firewalls, Other Gateways and Anti-Spam Tools:
 - 2.1. GCBH BH-ASO Primary Control at the Gateway Level:
 - 2.1.1. Install e-mail gateway antivirus software configured for full-time active mode;
 - 2.1.2. Configure anti-virus software to check/scan all files;
 - 2.1.3. Filter all arriving (and departing if possible) e-mail traffic by subject line /header;
 - 2.1.4. Be prepared to rapidly adjust filtering rules based on security notices, software vendor alerts, user reports, etc.
 - 2.1.5. Regularly review quarantined e-mails to determine whether or not to allow, delete, or block emails caught by e-mail gateway.
 - 2.1.6. Maintain whitelist/blacklist for e-mail gateway
 - 2.2. Gateway Level, Virus Prevention:
 - 2.2.1. Filter all arriving and departing e-mail by spam threshold (greater than 40 identical messages blocked and source traced, if inside);
 - 2.2.2. Filter messages that do not meet at least one method of DNS authentication (DMARC, SPF, or DKIM);
 - 2.2.3. Filter all *.exe attachments and similar;
 - 2.2.4. Filter all *.pdf and similar attachments;
 - 2.2.5. Filter ActiveX[®] and JavaScript[®].
 - 2.3. Human Factors Virus Prevention:
 - 2.3.1. Educate users to consider e-mail attachments and links potentially dangerous and to treat them very cautiously. Specifically recommend education: Open only expected attachments and links from known and trusted sources. Delete or question all others before opening;
 - 2.3.2. Keep system managers updated and informed;
 - 2.3.3. Reinforce the message to users to never double click an e-mail attachment that is not expected. This policy is difficult since the affected (malicious) email will

normally come "From" a trusted person. (Well informed users can be taught that *.docx, *.exe, *.pdf, *.html, *.vbs, and *.hta extensions are the most likely to be dangerous). Desktop anti-virus software will normally work if it is kept updated and properly configured to operate full-time in the background;

2.3.4. Users that experience more than 2 anti-virus alerts in a 30-day period may be categorized as "high risk" users. Depending upon the source and nature of the infection, High Risk users will be subject to the following policy:

2.3.4.1. Disabling of email and/or Internet access; and

2.3.4.2. Disabling of external drives such as USB devices, etc.

APPROVAL



Karen Richardson or Sindi Saunders, Co-Directors

7/8/24
Date