Effective Date: 7/1/2019
Review Date: 9/26/2023
Revised Date: 9/5/2023

North Sound Behavioral Health Administrative Services Organization, LLC

Section 4000 - Information Systems: Malicious Software Prevention

Authorizing Source: HCA Contract
Approved by: Executive Director Date: 9/26/2023 Signature:

POLICY #4007.00

SUBJECT: MALICIOUS SOFTWARE PREVENTION

POLICY
This policy is designed to protect North Sound Behavioral Health Administrative Services Organization (North Sound BH-ASO) equipment and networks from the potent threat of software viruses, spyware intrusion and infection.

1. **Desktop Systems**

   North Sound BH-ASO Primary Controls at Desktop Anti-Virus Level. These controls will be implemented by the IT Department unless otherwise indicated.

   a. Certified anti-virus software will be installed on all desktop and laptop PCs, workstations, and Servers.

   b. Subscribe to antivirus alerting and virus definition update services provided by the software vendor. Continuous monitoring of the software vendor's site for updates will be the responsibility of the IT Department.

   c. Desktop anti-virus software (signatures) will be updated automatically using automated processes. No user intervention will be required. The automatic updates will be monitored by the IT Department.

   d. Implement the following desktop/laptop/workstation anti-virus software configuration:

      a. Enable full-time, background, real time, auto-protect or similar mode.

      b. Enable start-up scanning of memory, master / boot records, system files.

      c. Configure scanning/checking options to include checking for all files.

      d. Enable logs for all desktop virus-related activity.

   e. Subscribe to alert services from office productivity suite vendors and install all recommended security updates automatically, or via network software policies.

      i. Additional notes on desktop level policies

         a. Alerts to users are neither recommended nor discouraged. However, system administrator alerts, logs, or other advisories are to be continuously enabled. Users shall not forward virus warnings received from sources other than the Security Officer or IT Department as they may be hoaxes. Any virus warning received from other sources should be verified by the Security Officer or IT Department to verify its authenticity.

         b. User controls over the anti-virus software will be set to require elevated access to prevent users from inadvertently disabling anti-virus protection.

         c. User-driven scanning of removable media, downloads or hard drives are not required as anti-virus software will be configured to perform these functions automatically. However, now that all North Sound staff are primarily remote teleworkers, it is recommended that staff familiarize themselves with the process and get in the habit of scanning downloads and removable drives as an added layer of security.

North Sound BH-ASO Recommended Synergistic Controls at the Desktop-Level. These controls will be implemented by the Security Officer or the IT Department unless otherwise indicated.

a. Enable Macro Virus Protection in Microsoft Office© Programs.
b. Use the anti-virus software heuristic controls (in full-time background mode where available).
c. Synergistic Controls at the E-Mail Client Level.
d. Turn off auto-open attachments.
e. Configure email clients to convert email messages to “plain text” or PDF format.
f. Configure to block execution of all executable attachments (e.g.: *.EXE, *.HTA, *.VBS, etc.), as well as other attachments known to pose a security risk.
g. Configure to challenge opening of other attachments that could pose a security risk.
h. Configure to challenge double click of all attachments.

2. **Network File and Print Servers**

a. Primary Control at Server level.
b. Run anti-virus scanner in full time, background, automatic, auto-protect or similar mode on any file server which potentially stores files which are potentially at risk for infection such as *.doc files and executables which run on desktops.
c. Update server Antivirus signatures as notified via software vendor’s subscription service.

i. Synergistic Controls at the Server Level

a. Utilize centralized anti-virus management.
b. Utilize centralized desktop management.
c. Manage web browser and scripting centrally.

3. **E-Mail Gateways, Firewalls and Anti-Spam Tools**

a. **Primary Control at the Gateway Level**

i. Install firewall patches and updates as soon as possible after they are released, or at the next available maintenance window.
ii. Install e-mail gateway antivirus software configured for full-time active mode.
iii. Configure anti-virus software to check/scan all files.
iv. Configure to block execution of all executable attachments (e.g.: *.EXE, *.HTA, *.VBS, etc.), as well as other attachments known to pose a security risk.
v. Filter all e-mail traffic for known viruses if possible.
vi. Be prepared to rapidly adjust filtering rules based on security notices, software vendor alerts, user reports, etc.
vii. Filter all arriving email traffic for spam and phishing related content.

b. **Gateway Level, Potential Synergistic Controls**

i. Filter all arriving e-mail by spam threshold.
ii. Block all executable attachments.
iii. Block all known phishing messages.
iv. Filter all Microsoft Office (*.docx, etc.) and similar attachments.
v. Filter ActiveX©, Java and JavaScript© attachments.

c. **Human Factors Potential Synergistic Controls**

i. 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.

ii. 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 often appear to come "From" a trusted person. Desktop anti-virus software will only work if it is kept updated and properly configured to operate full-time in the background.

iii. Educate users to never download files from unknown or suspicious sources (e.g., websites, email messages, etc.).

4. **Points of Contact**

Questions about this policy may be directed to the Security Officer or IT Support.

5. **Enforcement**

All managers are responsible for enforcing this procedure. Employees who violate this procedure are subject to discipline up to and including termination from employment in accordance with North Sound BH-ASO's Employee Conduct and Discipline policy.

ATTACHMENTS

None