Effective Date: 6/28/2005
Revised Date:
Review Date:

North Sound Mental Health Administration

Section 4000 – Information Systems: Malicious Software Prevention

Authorizing Source:
Cancels:
See Also: Approved by: Executive Director Date: 6/28/2005
Responsible Staff: IS Specialist Motion #:

POLICY #4007.00

SUBJECT: MALICIOUS SOFTWARE PREVENTION

POLICY

This policy is designed to protect NSMHA equipment and networks from the potent threat of software virus and spyware intrusion and infection.

A. Desktop Systems

NSMHA Primary Controls at Desktop Anti-Virus Level. These controls will be implemented by the IS/IT Department unless otherwise indicated.

1. Install certified anti-virus software on all desktop and laptop PCs and workstations.
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 the IS/IT Department.
3. Desktop anti-virus software (virus signatures) will be updated automatically through the use of network software policies. No user intervention will be required. The automatic updates will be monitored by the IS/IT Department.
4. 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

5. Subscribe to alert services from office productivity suite vendors and install all recommended security updates automatically through the use of network software policies.

a. Additional notes on desktop level policies

i. 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 IS/IT Department as they may be hoaxes. Any virus warning received from other sources should be verified with the IS/IT Department to verify it's authenticity.

ii. User controls over the anti-virus software will be set to minimum levels to prevent users from inadvertently disabling anti-virus protection.

iii. User-driven scanning policies such as requesting users to scan floppies, downloads or hard drives are not recommended as they are generally more expensive and infringing

than useful. To that end, anti-virus software will be configured to perform these functions automatically.

NSMA Recommended Synergistic Controls at the Desktop-Level. These controls will be implemented by the IS/IT Department unless otherwise indicated.

i. Enable Macro Virus Protection in Microsoft Office© Programs
ii. Use the anti-virus software heuristic controls (in full-time background mode where available)
iii. Synergistic Controls at the E-Mail Client Level
iv. Turn off auto-open attachments
v. Configure email clients to convert email messages to "plain text" format
vi. 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.
vii. Configure to challenge opening of other attachments that could pose a security risk.
viii. Configure to challenge double click of all attachments

B. Network File and Print Servers

1. Primary Control at Server level
2. 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.
3. Update server signature as notified via software vendor's subscription service/alert service.

a. Synergistic Controls at the Server Level

i. Utilize centralized anti-virus management
ii. Utilize centralized desktop management
iii. Manage Internet Explorer© and Visual Basic© Scripting centrally

C. E-Mail Gateways, Firewalls, Other Gateways and Anti-Spam Tools

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

a. Install e-mail gateway antivirus software configured for full-time active mode.
b. Configure anti-virus software to check/scan all files
c. 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.
d. Filter all arriving and departing e-mail traffic by subject line /header for known viruses if possible
e. Be prepared to rapidly adjust filtering rules based on security notices, software vendor alerts, user reports, etc.
f. Filter all arriving email traffic for spam and phishing related content.

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

   a. Filter all arriving e-mail by spam threshold
   b. Block all executable attachment
   c. Block all known phishing messages
   d. Filter all *.doc and similar attachments
   e. Filter ActiveX© and JavaScript©

3. **Human Factors Potential Synergistic Controls**

   a. 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.
   b. 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. Desktop anti-virus software will normally work if it is kept updated and properly configured to operate full-time in the background.
   c. Educate users to never download files from unknown or suspicious sources (e.g., websites, email messages, etc.).

D. Contact point

Questions about this policy may be directed to the IS Specialist.

E. 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 NSMHA's Employee Conduct and Discipline policy.

ATTACHMENTS

None