



THE CITY OF NEW YORK
DEPARTMENT OF INFORMATION TECHNOLOGY & TELECOMMUNICATIONS

ANTI VIRUS SECURITY POLICY

THE POLICY

CITY OF NEW YORK COMPUTING RESOURCES WILL BE PROTECTED FROM MALICIOUS SOFTWARE AND VIRUSES.

SCOPE

This policy applies to all computer systems that access or process City information

MONITORING

- 1) DoITT in conjunction with the agency CISO reserves the right to scan the network and computing resources for malicious software including but not limited to viruses¹ or spyware².
- 2) DoITT reserves the right to quarantine any agency network or computing resource that may pose a risk to Citynet.
- 3) DoITT reserves the right to immediately disconnect from Citynet any device inadequately protected by anti-virus or anti-spyware software.
 - a. Computing devices removed from Citynet for non-compliance must confirm appropriate remediation prior to reconnection to Citynet.

ANTI-VIRUS REQUIREMENTS

- 4) Servers, desktops, and laptops must have commercial anti-virus software installed, properly configured and running at all times
- 5) Anti-virus software must be configured to automatically remove the virus
- 6) Users shall not disable automatic virus scanning on their local machines
- 7) Server administrators will not disable anti-virus software on server machines.

ANTI-VIRUS & SPYWARE SCANNING

- 8) Users should not initiate any scans on devices beyond their local resources (e.g. hard disk, CD, USB). Users will refrain from scanning network resources.
- 9) All electronic mail entering and leaving Citynet (i.e., to/from the Internet) must be scanned.
- 10) Electronic mail entering or leaving Citynet may be blocked on the basis of file type and file size.

¹ Software used to infect a computer

² Software that sends information about your Web surfing habits back to its Web site



THE CITY OF NEW YORK
DEPARTMENT OF INFORMATION TECHNOLOGY & TELECOMMUNICATIONS

- a. The criteria for blocking of items are maintained by DoITT and shall be reviewed and updated periodically as circumstances require.
- 11) Scan settings for laptops, desktops, workstations that are not explicitly addressed by this policy shall be determined by the agency level CISO.

ANTI-VIRUS UPDATING

- 12) Agency administrators are responsible for validating version and signature files for desktop and laptop machines.
- 13) Server administrators are responsible for validating version and signature files for servers.
- 14) Users are responsible for validating version and signature files for stand-alone computers that are not connected to the network.
- 15) When possible, signature updates must be installed without user intervention.
- 16) New versions of the virus signature files must be loaded within 48 hours. Failure to comply will result in disconnection from Citynet.

VIRUS REPORTING

- 17) If an agency is hosted by DoITT users must notify the DoITT helpdesk when a computer virus is suspected or detected. All other agencies should notify their local information technology team.
- 18) All virus alerts must be followed by an immediate full scan of affected devices performed by IT personnel.
- 19) Agency administrators must perform a root cause investigation when a virus is identified to ensure proper containment.

USER RESPONSIBILITIES

- 20) Users should not open any files attached to electronic mail from an unknown or un-trusted sources. Electronic messages with suspicious subject lines or content should be deleted without opening.