Anti-Virus Security Policy

The Policy

City of New York computing resources must be protected from malicious software and viruses.

Scope

This policy applies to all Mayoral agencies and to all systems residing on CityNet.

Monitoring

1) DoITT and the respective agency CISO may scan the network and computing resources for malicious software including but not limited to viruses,[1] malware[2] and spyware.[3]

2) DoITT may, in order to preserve the overall security of Citynet, quarantine any agency network or computing resource that is disruptively infected with viruses, malware or spyware.

Anti-Virus Requirements

3) All servers, desktops and laptops connected to Citynet, including those on agency networks which are connected to Citynet, must participate in the Citywide managed anti-virus security cloud.

4) End users shall be prevented from disabling the anti-virus agent installed on City provided computing resources.

5) Authorized administrators may temporarily disable the anti-virus agent for trouble-shooting and/or software installation purposes and must immediately re-enable anti-virus scanning upon completion of trouble-shooting/installation.

Email Requirements

6) All electronic mail entering and leaving Citynet (i.e., to/from the Internet) must be scanned for viruses and malware.

7) Electronic mail entering or leaving Citynet may be blocked on the basis of detected spam, threats and/or IP reputation.

Anti-Virus Updating

8) Agencies shall assign responsibility for validating version and signature files for stand-alone computers that are not connected to the network.

9) When possible, signature updates must be installed without user intervention.

10) New versions of the virus signature files must be loaded within 48 hours.

---

[1] Software used to infect a computer.

[2] Software designed to interfere with normal computer functions and/or send information to unauthorized parties.

[3] Software that sends information about your Web surfing habits to unauthorized parties.

Virus Reporting

11) Agencies not directly connected to Citynet must report virus and worm outbreaks immediately to the Citywide CISO, following the Citywide Incident Response Policy. A virus outbreak is considered to be the detection of the same virus on 5 or more workstations within a 3 hour period.

User Responsibilities

12) In order to protect against malicious code, users should be cautious opening any files attached to electronic mail from unknown or un-trusted sources. The legitimacy of any suspect messages should be verified by contacting the sender through an alternate channel such as a direct conversation or a phone call.

Compliance

13) DoITT reserves the right to immediately disconnect any device or agency from Citynet which it deems out of compliance with this policy.

Document Revision History

Date	Description
July 28, 2008	**Version 1.1** issued.
June 16, 2011	**Version 1.2** Updated header with new NYC logo and added this revision history table to the document.
Sep 21, 2012	**Version 1.3** Updated to reflect the introduction of the Citywide managed anti-virus security cloud, bullet 3. Updated various bullets for greater clarity.
Sept. 9, 2014	**Version 1.4** Policy review and minor formatting updates.