City University of New York
Information Technology Policies, Standards & Guidelines

Anti-Virus Software Policy

Approved by the Information Technology Steering Committee on:

December 18, 2003

Policy Number:
2003-003
AntiVirus Software Policy

Approved by the City University of New York IT Steering Committee on December 18, 2003

The internal computers systems, networks and data repositories of The City University of New York are critical resources of the University and its Colleges and must be protected against unauthorized access, malicious access, and disruption of service. Active measures are necessary to lessen the opportunity for such incidents.

In order to reduce the opportunity for introduction of viruses, worms and Trojan Horses, all student, faculty, and staff desktops, workstations, laptops/notebooks and servers running Windows, Macintosh or UNIX operating systems, and which are either physically or remotely connected to the City University network will have a passive anti-virus detection and removal application installed and active on those desktops, workstations, laptops/notebooks and server. Users are responsible for ensuring that anti-virus files are kept up to date.

Each College and Central organizations Information Security Officers (ISO) are responsible for monitoring compliance by their respective users with this policy and associated standards by: (1) directing administrators of Windows©, Macintosh© and UNIX machines in their respective organizations that are provided by the University/College and connected to the University/College network to install approved anti-virus software; (2) directing reviews of, and action on, reports on compliance with this policy that are generated by CUNY IT Steering Committee’s Security & Disaster Recovery sub-committee. Individual users are responsible for compliance with this policy and its associated standards for personal machines connected to the University/College network and (3) implement a central anti-virus server system at the head end to check all emails for viruses and clean them if infected.

The Standards sub-committee will provide recommendations to the Security & Disaster Recovery sub-committee for the development and revision of standards. Both these sub-committees will forward recommendations for changes and rationales for the changes to the CUNY IT Steering Committee for consideration of future updates and funding. Instruction and assistance on installation and maintenance of anti-virus software will be developed and offered by College and Departmental IT contacts in coordination with the respective ISOs.

This policy becomes effective on December 18, 2003.
Rationale

Rising frequency of security incidents involving network-attached devices significantly increases the probability of major disruptions to the internal computer systems of the University/College. Statistics indicate that a very large percentage of potentially damaging incidents can be avoided by the use of existing anti-virus detection and elimination procedures. Establishing policy centrally and issuing standards and utilities from a central authority allows for rapid incident response and continuous update of protection methods.

Standards

Anti-Virus Software: The University provides a CUNY wide license contract for an Anti-Virus software as selected by the IT Steering Committee that each college can use for purchasing. This application when installed using ISO provided instructions allows for the least amount of interruption or activity required from end users. Installation should be configured for automatic scanning and automatic updates. Users who know of or expect interference between the anti-virus software and another applications running on their workstations or laptops must contact the Information Security Officer to evaluate and agree on work-arounds.

Submitted by the Security & Disaster Recovery Subcommittee to the full IT Steering Committee on November 20, 2003.