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

Anti-Virus Software Standards

Approved by the Information Technology Steering Committee on:

July 31, 2002

Policy Number:

2002-004
CUNY Standard for Virus Protection

Since receiving its initial charge from the Chair of the CUNY Information Technology Steering Committee, the Subcommittee on Standards has sought to frame recommendations on Information Technology, IT, standards that:

- capitalize on de facto standards, where appropriate
- suggest adjustments to existing practices, where needed
- facilitate the establishment of standards in emerging technologies where University policies and practices are still in development.

To achieve these objectives, a series of short-term and long-term goals were set. These included identifying existing data that would guide recommendations, proposing methods for gathering information where critical gaps exist, and addressing issues that afford the University and individual institutions the opportunity to leverage their purchasing power.

Central to the approach taken by the committee was to advance proposals focused on functional requirements rather than vendor-specific feature sets. To date, this has driven draft recommendations on desktop computing standards and has spawned related activities on telecommunications in general and voice over IP in particular. In the diverse realm of software, however, the issues are both more numerous and complicated.

Given the wide range of software packages in use throughout CUNY, the Subcommittee elected to focus on an area where the University could both realize immediate benefits and establish a framework for instituting standards in other software applications. The disparity in unit pricing throughout the University, coupled with the number of packages in use, made virus protection software a logical point of departure.

The recommendations of the Subcommittee that follow seek to establish a CUNY Standard for virus protection. The proposal is comprised of six sections:

1. Virus Protection Policy and Responsibilities
2. Technical Specifications
3. CUNY Volume Discounts
4. Implementation Procedures
5. Review Process
6. Exceptions

1. Virus Protection Policy and Responsibilities
As a basic proposition in network security, all desktop computers and servers used throughout CUNY must have, and regularly use, virus protection software to prevent the introduction or propagation of viruses. While this would seem to be self evident, current information would suggest that this practice is not as routine as it needs to be. Training
must take place to ensure that all computer users know and understand safe computing practices. As a corollary to user practices, institutions should ensure that virus protection software is kept current.

2. Technical Specifications
A CUNY Standard for virus protection must meet minimum requirements for technical specifications and features. It should:

- be recognized throughout the IT industry as a leader in virus protection
- be schedulable for automatic virus definition updates and scanning
- provide auto protect features for viruses including e-mail viruses
- provide timely updated virus definition in line with the best available in the IT industry
- seamlessly integrate with a server based virus protection product.

In addition, the CUNY Standard should not only provide competitive pricing but also provide additional discounts beyond those from New York State, GSA or similar contract pricing for CUNY-wide volume purchases.

3. CUNY Volume Discounts
A review by the University Computer Center, UCC, technical support group confirmed that, while a number of virus protection packages are in use throughout the University, only a limited number meet the criteria proposed above. Recent vendor negotiations conducted by the UCC group further reduced the number of virus protection software packages that met the CUNY standard proposed here. The following products, therefore, are recommended:

- McAfee – Virus Secure Suite,
- Norton – Anti-Virus.

4. Implementation Procedures
The ability of CUNY units to avail themselves of the benefits of volume pricing is crucial to the adoption of a University wide standard. In order to facilitate volume purchasing and ensure the maximum savings University-wide, the subcommittee recommends that a procedure be developed with the above vendors that permits all CUNY units to purchase this software at volume pricing rates. Examples of possible methods for administering this process are:

- A CUNY account number issued by a vendor. This account number would be provided to the vendor by the CUNY unit making the purchase with each purchase order. The vendor would provide the volume pricing and record the details of the transaction for later review and accounting of the total number of licenses purchased by the University. This information could be used in future volume pricing negotiations.
- A CUNY wide purchase would be coordinated by the University central administration. Participating CUNY units interested in purchasing products at that time specify the quantity and the associated funds would be transferred as “book entries”. The distribution of the software and or
licenses would be coordinated centrally. The purchasing process should be repeated frequently enough to ensure the volume discount savings and minimum delay in the availability of products for out-of-cycle purchasing. The frequency of purchasing and reorder quantities are parameters which should be fine-tuned based on inventory analysis which includes the representative overhead cost associated with the CUNY-wide purchase and the threshold quantities required for volume discounts.

5. **Review Process**

It is axiomatic in the IT field that what is state of the art today is likely to be obsolete tomorrow. It is, therefore, imperative that the CUNY standard for virus protection be reviewed at least once each year by the Subcommittee on Standards. Adjustments or modifications necessitated by advances in the technology should be made to the standard as soon, as is practical.

6. **Exceptions**

Accommodations may need to be made to address the unique needs of an institution or of a specific set of users within the University. In such cases, users should submit requests for exceptions to be reviewed by the Subcommittee on Standards. Exemptions will be granted with the proviso that alternatives to the standard are cost effective and provide virus protection solutions equivalent to, or better than, the guidelines cited in items 2 and 3 above.

This policy was approved by the IT Steering Committee July 31, 2002.