



## Antivirus Software Policy

### Purpose

To provide guideline for the use of Anti-Virus Software at Albany State University

### Policy

All student, faculty, and staff desktops, workstations and laptops/notebooks, running Windows or Macintosh operating systems, and which are either physically or remotely connected to the Albany State University network will have a passive anti-virus detection and removal application installed and active on those desktops, workstations and laptops/notebooks.

### Scope

This policy applies to all students, faculty, and staff who have desktop, workstations and laptops/notebooks which are either physically or remotely connected to the Albany State University network. This policy also applies to contractors and temporary staff whose personal laptops will connect to the Albany State University network (if applicable).

### Terms

**Antivirus software** consists of computer programs that attempt to identify, thwart and eliminate computer viruses and other malicious software by examining (scanning) files to look for known viruses matching definitions in a virus dictionary and/or identifying suspicious behavior from any computer program which might indicate infection.

### I. Introduction

The internal computers systems, networks and data repositories of Albany State University are critical resources of the University and must be protected against unauthorized access, malicious access, and disruption of service. Active measures are necessary to lessen the opportunity for such incidents. Rising frequency of security incidents involving network-attached devices significantly increases the probability of major disruptions to the internal computer systems of the University. 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.

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



## II. Standards

**Faculty and Staff Employees:** The University provides a site-wide license for Symantec (Norton) Anti-Virus, which is available to all faculty and staff members. This application, when installed using OIT-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 application running on their workstations or laptops must contact the University Security Officer to evaluate and agree on work-arounds.

**Individual users (including but not limited to students, guests, contractors, and temporary employees):** Individual users must procure their own anti-virus software for use on a personal computer which will be connected to the ASU network. It is the responsibility of the individual user, in conjunction with their respective supervisor, to ensure that all University-owned computers on which they work have up-to-date anti-virus installed and configured.

## III. Compliance

**Faculty and Staff Employees:** Vice-Presidents, Administrative Unit Directors, and Deans are responsible for monitoring compliance by their respective users with this policy and associated standards by:

- a. Directing administrators of Windows© and Macintosh© machines in their respective organizations that are provided by the University and connected to the University network to install approved anti-virus software
- b. Directing reviews of and action on, reports on compliance with this policy that are generated by Office of Information Technology

**Individual users (including but not limited to students, guests, contractors, and temporary employees)** are responsible for compliance with this policy and its associated standards for personal and University-provided machines connected to the University network.

## IV. Revision of Policy

College and Departmental IT contacts will provide recommendations to OIT for the development and revision of standards. OIT will forward recommendations for changes and rationales for the changes to the Campus Technology Committee for consideration of future 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 OIT.