California State University Northridge	**Information Technology** Computing Device Anti-Virus Software	**Page** 1 of 2	
		SOP#: 500-01	**Revision#:**

Prepared by: Unknown **Date:** October 11, 2004	**Approved by:** Previously approved by President as policy 500-01 **Date:** October 11, 2004
Last revised by: Chris Olsen **Date:** November 7, 2011	**Last approved by:** Chris Olsen, ISO **Date:** November 7, 2011

1.0 INTRODUCTION

On a daily basis, the campus is exposed to a large number of electronic viruses. Although the campus e- mail environment has an antivirus filter, viruses can also be transmitted in other ways, for example, through file sharing and downloading. Once infected with a virus, a computing device is susceptible to a greater number of electronic attacks. The virus and subsequent attacks can, for example:

- Render the computing device unusable
- Spread itself from this device to other devices
- Use the device to participate in further electronic attacks
- Allow unauthorized to access to both the device and the protected data it contains

Antivirus software is an effective step to reduce the Campus's vulnerability associated with software viruses. To be effective, all campus computers must be appropriately protected.

2.0 PROCEDURES

All computing devices attached to the University network must run antivirus software with up-to-date virus definitions and that conforms to University standards or must be protected by other appropriate means. The settings for the virus protection software must not be altered in a manner that reduces the effectiveness of the software.

- Each deployment of antivirus software shall be configured to ensure automatic updates of virus definitions based upon the following criteria:
  - On campus, university-owned computers shall be updated via either the Enterprise or a local virus definition server.
  - On campus, privately-owned computers, e.g., students in Residence halls, shall be updated via a live update to the vendor supplied virus definition server.
  - Off-campus computers shall be updated via a live update to the vendor supplied virus definition server.

- Any campus user who detects a virus, in accordance with the Campus Information Security Response Procedure, must notify their local technical administrator, or the Help Center, or the Information Security department (security@csun.edu) to report the incident. Unfiltered virus constitutes a security incident and must be reported.
- A computer that is either unprotected by antivirus software or by other appropriate means, or is infected may be removed from the network.

3.0 APPLICABILITY AND AREAS OF RESPONSIBILITY

- Local IT units are responsible to ensure antivirus software and automatic updates of virus definition files are properly installed and configured on University-owned computers. The owner of a privately owned computer is correspondingly responsible for his or her computer.
- Vice Presidents and Deans are the point of accountability for ensuring that personnel adhere to this policy.
- Information Technology (IT) shall provide support to local IT units in the following ways:
    - IT is responsible for maintaining an Enterprise Antivirus Server from which automatic updates of virus definition files can be automatically obtained.
    - IT is responsible for coordinating with college IT units to provide appropriate antivirus software.
    - IT is responsible for disconnecting unprotected or infected computers from the network.

4.0 RESOURCES AND REFERENCE MATERIALS

500-08 Security Attacks

500-10 Use of Computing Resources

500-8045 Network Security and Security of Devices Connecting to the Network