SOFTWARE ANTIVIRUS POLICY

1.0 PURPOSE

This document provides the policies for preventing, detecting, removing, and the reporting of malicious computer software, such as computer viruses. The purpose is to assure that pro-active security measures are taken to prevent malicious software from occurring; to raise awareness for recognizing and immediately reporting the occurrence of malicious software; and to ensure that appropriate action is taken to minimize the consequences of a malicious software attack.

All users are expected to understand the danger that viruses can cause to individual company computers as well as the entire network. All computers (clients and servers) connected to the computer network (herein referred to as "the network") or networked resources shall have IT department supported antivirus software correctly installed, configured, activated, and updated with the latest version of virus definitions before or immediately upon connecting to the network.

If deemed necessary to prevent the propagation of viruses to other networked devices or detrimental effects to the network, computers infected with viruses or other forms of malicious code (herein collectively referred to as "virus" or "viruses") shall be disconnected from the network until the infection has been identified and removed.

2.0 SCOPE

The policy contained in this document is applicable to all information and infrastructure computing resources, at all levels of sensitivity. This policy is mandatory for all employees, contractors, and others who process, store, transmit, or have access to IT information and infrastructure computing resources. This policy applies to all existing automated systems and to any new systems technology acquired in the future. This policy applies to all operating system environments.

3.0 POLICY

The IT department shall ensure that all computers on the network have IT Department supported antivirus software installed. If a computer does not have IT Department supported antivirus software installed, it shall be installed according to one of the two following methods:

- If the installation source is a distributed disk, the antivirus software shall be installed before establishing any connection to the network. Upon establishing the initial network connection, the virus definitions shall be updated to the most current version immediately and before loading or installing any other software or data.

- If the installation source is a local server, the computer shall be connected to the network for the sole purpose of installing antivirus software from that server. The installation shall be performed immediately upon establishing the initial network connection and virus updates downloaded and installed before loading or installing any other software or data.

Under all other circumstances, any computer connected to the network, including servers, shall have IT Department supported antivirus software properly installed, configured, and updated before being connected to the network. IT Department will ensure that:

- Virus definitions will be updated at least once every 12 hours

- All files on all hard drives will be scanned daily for viruses.

When an enterprise-wide virus attack is in progress, the IT Department shall notify the computing community via the best available method and all files on all hard drives should be scanned immediately using the newest virus definitions available.

Other operating systems or computing platforms shall have comparable protection, if available. In the event that no antivirus protection is available for a particular operating system or platform, anyone using or accessing these unprotected systems shall apply all prudent security practices to prevent infection, including the application of all security patches as soon as they become available. When antivirus software becomes available for an operating system or platform previously lacking antivirus software, it shall be installed on all applicable devices connected to the network.

3.1 JUSTIFICATION AND RATIONALE

Availability, performance, and security of the network represent essential core assets to data integrity, security and the daily operations. Viruses and other forms of malicious code (malware, worms, trojans, backdoors, VBS scripts, mass-mailers, etc.) represent a significant threat to these assets. In order to combat this threat, a comprehensive enterprise security policy must include antivirus provisions to detect, remove, and protect against infections. Antiviral procedures should include identification of current and potential viral threats, computers and systems at risk of infection, files at risk of infection, infected computers, and infected files. Infection patterns should be tracked and analyzed to identify chronic internal and external threats.

Many virus infections threaten other computers sharing the infected computer's network. Infected computers must be cleared of viral infections immediately. Files that can be cleaned should have the viral code removed, thus returning them to pre-infected state. Files that cannot be cleaned must be quarantined until such time as they can be replaced with uninfected copies. If all efforts at removing viral infection fail, the computer's hard drive must be formatted and all software reinstalled using clean licensed copies. If an infected computer is deemed capable of infecting or affecting other computers or the network, the infected computer must be disconnected from the network until it is serviced by an IT Department representative or designee who will verify that the computer is virus-free.

Antivirus activities must be centrally managed. New viruses represent a continual threat, requiring continual research to plan proactive measures against them. Users must be educated about viral threats and the computing practices required to protect against infections. Whenever a new viral threat appears, the user community must be warned about the new threat. Up-to-date antivirus software must be distributed and its availability advertised to the users.

3.2 ESTABLISHED ANTIVIRAL PROCEDURES

Every year, IT department purchases licenses for an enterprise level antivirus software package to protect computers and systems from virus infections. Computers purchased for large-scale deployments may be delivered with antivirus software already installed. Whenever IT Department personnel set up a new computer, they ensure that antivirus software is installed before, or immediately upon, connecting the computer to the network.

IT department provides end-user support and forwards virus-related service requests (coded with high priority by default) to the appropriate group for rapid response. IT Department provides enterprise-level antivirus support and coordination of rapid responses to enterprise-level virus attacks.

REVISION HISTORY

Release No.	Date	Revision Description

REVIEW SCHEDULE

None

OWNER

CIO

DELEGATED OWNER