Anti-Virus Software Policy

Date: 06/05/06	**Policy ID:** UVAW-5	**Status:** Approved

Contact Office: Office of Information Technology

Oversight Executive: Director of Information Technology

Applies to: All systems connected to the College network (College or privately owned)

Reason for Policy: For the protection of data, information, and resources connected to the UVa-Wise College network.

Definitions:

Policy Statement: Operating systems, application software, all software is susceptible to malicious scripts, viruses, worms, trojan horses, etc. Vulnerabilities built into the software either consciously or inadvertently becomes prime candidates to be targeted. Anti-virus software is a proven method to help defend against such infestations.

Procedures:

1.0 Anti-Virus Software, updates and definitions
- 1.1 All systems commonly affected by viruses (including PCs and servers) that attach to the College network (whether College-owned or privately-owned) must have anti-virus mechanism(s) in place.
- 1.2 All anti-virus mechanisms must be current (receiving updates automatically), actively running, and generating audit logs.

2.0 All College-owned PC's will have Norton (Symantec) Anti-Virus loaded onto the systems and set for automatic updates.
- 2.1 The Norton (Symantec) Anti-Virus Server log will be reviewed weekly and systems suspected of viruses will be subsequently scanned and cleaned. (If a system cannot be cleaned by removal tools, etc. the system will be "wiped" and rebuilt.)

Related Information: See also Anti-Virus/Critical Update Policy PCI – 5

Background: Approved by Brian Ward, CIO – UVa-Wise, June 5, 2006
