This policy will help ensure that all vulnerable computing platforms in the College of LSA are hardened against attack and protected by anti-virus software at all times.
# Contents

Purpose and Rationale ............................................................................................................. 1  
Anti-Virus Software Policy Statement .................................................................................... 1  
System Hardening and Anti-Virus Software Management .................................................... 2  
Standards & Procedures ........................................................................................................ 2  
Questions Regarding this Document ..................................................................................... 3
Purpose and Rationale

- The College of LSA shall promote a secure computing environment for all students, faculty, staff and affiliates. Computing platforms (including but not limited to: desktop workstations, laptops, hand-helds, personal digital assistants, servers and network devices) are integral elements in the operations of the College and as such are vital to the College's mission. Computer viruses, worms, trojans, etc. constitute a major threat to the integrity and performance of the computing operations on campus, including access to critical data and the availability of the campus network. This policy will help ensure that all vulnerable computing platforms on campus are hardened against attack and protected by anti-virus software at all times. The rising frequency of security incidents involving network-attached devices significantly increases the probability of major disruptions to the internal computer systems of the College and University at large. 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 from a central authority allows for rapid incident response and continuous update of protection methods. As part of a ‘Defence in Depth’ strategy to continue to secure computers across the College, from this point on, all Windows and Macintosh computers will require that Anti-virus (AV) software be installed and running. Furthermore, that the software be configured to regularly download updates and new AV signature files – either automatically on release from the AV Support or within a 48 hour period (refer to regular Business Hours). At this point, Linux systems are to be considered an exception to this policy except for those systems which may provide services (file/print or email for example) to Windows and/or Macintosh systems. Furthermore, University Audit completed an audit of research computing in the College of LSA during the Summer of 2010. One of the areas of concern targeted by this audit was the lack of Anti-Virus software on older, operating systems/hardware still being used for research operations. The audit also pointed out that some LSA departments were solely relying on the College’s IT Security Policy (written updated and approved by LSA Leadership 10/05). The presence of sensitive data certainly requires further defining of IT Security Policy for research computing in these areas. However, it is also known fact that the College deals with sensitive data in other forms besides research data – Human Resources data, Personally Identifiable Information like Social Security numbers, etc. The overarching LSA IT Security Policy may not contain enough detail or include appropriate restrictions to apply to areas that involved sensitive or critical data, therefore, this document is being written in hopes of addressing this problem.

Anti-Virus Software Policy Statement

- Any computer or network device connected to the College of LSA’s network shall be protected from malicious electronic intrusion by anti-virus software. This policy applies to all devices connected, by any means (including wireless or dial-up connections), to the LSA network including those owned by the University, private individuals such as faculty, staff and students, affiliates, and third-party vendors. This includes any systems obtained through University’s start up funds, and internal/external grant funding. Passive anti-virus detection and removal applications will be installed and activated on all Windows and Macintosh desktops, workstations and laptops/notebooks which are either physically or remotely connected to the College of LSA’s network. You are allowed your choice of AV client but it must be from a reputable vendor. LSAIT encourages centrally managed AV client solutions although that is not a qualification and several excellent AV clients are available that are not currently centrally managed by the College. Autoupdate
settings for downloading new AV signatures must be configured such that the client downloads updates within a 48 hour period.

- Exceptions: Legacy OS systems connected to Instrumentation (these systems will not be connected to the Internet). Exception systems that must be connected to the network will not be allowed to browse the Internet nor do email as these are primary attack vectors for local compromise of the system. These systems, when shown to have incompatibilities that interfere with research, will be exempt – but only when the interference is demonstrated. This of course assumes that the AV software is configured properly and is working properly. Sometimes real-time scanning of files can be a problem, but in cases such as these, the solution can be to simply exclude particular directories – no need to uninstall altogether. In some cases, these legacy systems may need to connect to the vendor’s website to download updates to the software needed to run the device connected to the computer. In cases like this, a hardware-based Firewall will be installed between this computer and the network connection and configured such that this computer can ONLY connect to the vendor’s website. At this point, ‘smart phones’ will be considered an exception.

**System Hardening and Anti-Virus Software Management**

- All computers or networked devices shall have applicable operating system and application security patches and updates installed prior to initial connection to the network and within seven days of their availability on the vendor’s web site thereafter. Additionally, those systems for which anti-virus software is available shall have it installed and configured for effective operation prior to their connection to the campus network. Mail Servers must be configured with anti-virus software that disinfects all incoming and outgoing electronic mail and attachments regardless of operating system.

Unit administrators, system administrators, individual computer users such as students, faculty, staff, affiliates and third-party vendors are individually and collectively responsible for the anti-virus software and applicable operating system and software patches for devices under their control. For privately-owned devices connecting to the campus network, this responsibility lies with the primary user of that machine.

All anti-virus software shall be actively managed to ensure that the latest software updates and the virus signatures are installed. It is strongly recommended that the anti-virus software be configured to obtain these updates automatically and within 48 hours from either the anti-virus vendor, from a central departmental location or campus-wide source.

LSAIT reserves the right to review any device attached to the network (public or non-public) for adequate virus protection. LSAIT continues to reserve the right to deny access to the network to any device found to be inadequately protected. Additionally, LSAIT reserves the right to disable network access to any device that is insufficiently protected, or currently infected with a virus. Network access may be restored when the device has been cleaned and current anti-virus software and applicable operating system and application patches have been installed.

**Standards & Procedures**

- **Compliance.** The LSA Deans, department Chairs/Directors are responsible for monitoring compliance by their respective users with this policy and associated standards by: (1) 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; and (2) directing reviews of, and action on, reports on compliance with this policy that are
generated by the LSA.Security team or the UM University Audits and the UM Infrastructure and Information Assurance group. Individual users are responsible for compliance with this policy and its associated standards for personal machines connected to the College’s network.

- **Anti-Virus Software.** The University provides a site wide license for anti-virus software (Mcafee/Sophos at this time). This application when installed using ITS ('Virus Busters’) 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 their local IT Staff and/or the LSA.Security team to evaluate and agree on mitigation methods and/or work-arounds.

**Questions Regarding this Document**

May be referred to the IT Security Manager for LSA;
Christopher Brenner (cbrenner@umich.edu) 734-647-8213

Email: LSA.Security@umich.edu

LSA.Security's web site:

[http://www.lsa.umich.edu/lsait/lsa-sec-itam/security](http://www.lsa.umich.edu/lsait/lsa-sec-itam/security)

References: Washington State University, Georgia State University