The University of Mississippi Anti-Virus Policy

The purpose of this policy is to describe the responsibilities of individuals, departments and the Office of Information Technology (IT) in protecting University of Mississippi (UM) computer systems against virus infections. A virus is a piece of self-replicating code, most often a malicious software program designed to destroy or damage information on computers. Some viruses cause no damage, but a significant number are specifically designed to cause data loss. Potential sources of viruses include shared media such as floppy disks or CDs, e-mail (specifically, e-mail attachments), and documents downloaded from the Internet. A virus infection is almost always costly to the institution whether through the loss of data (possibly permanent), staff time to recover a system, or the delay of important work.

IT Responsibilities

- Negotiate campus site-licenses (PC and Mac) for virus protection software that result in cost-effective solutions for campus units. Communicate these solutions to departments. Provide an opportunity for departments to purchase licenses at a rate that corresponds to the number of computers in the department and reflects the discount achieved through bulk purchasing.
- Provide training to participating departments on virus protection.
- Work with participating departments to install virus software on all computers.
- For faculty and staff in departments that choose not to participate in the site-license option, make available an option for individual purchase, e.g., through the FTDC. In this case, the individual, not IT, will be responsible for installation.
- Assist individuals with recovery from infections by providing swift and accurate advice and assistance at the level the user and the situation require. This includes containment to stop the spread, disinfecting to clean the system, and the capture of incident information for future use. *Note that there will be a charge of $50 per visit for more than two visits to the same desktop to disinfect the system within a fiscal year*. Requests for assistance from departments that choose not to participate in the IT-negotiated solution will be given a lower priority than participating departments.
- Perform trend analysis to locate problem areas and identify high-risk users where special actions may need to be taken. In cases of risk to other campus systems, take appropriate action to thwart the spread of the virus (for example, block outgoing data from infected systems).
- Proactively notify the campus of viruses as soon as they are known to be in circulation.
- Pursue server-based solutions as they become available to stop the propagation of viruses through University systems and networks.

Departmental Responsibilities

- Ensure that all departmental computers are running current virus protection software either through the IT-negotiated solution (referred to in this policy as “participating departments”) or another option.

- Designate a local contact for departmental virus protection to assist in installation of virus protection software, education of the user community and virus response.
- Schedule a mandatory-attendance workshop for all departmental computer users (including student employees) in which IT staff and the departmental contact train departmental users on protecting their systems.
- Ensure that all lab computers and other shared systems are adequately protected and that someone in the department has been designated as being responsible for their maintenance.

Individual Responsibilities

- Update virus protection software frequently (weekly at a minimum).
- Configure desktop system to perform frequent auto-scans for viruses (daily recommended). Be sure to include any removable media in the scan.
- Install any recommended security patches for the operating system and applications that are in use.
- Exercise extreme caution when opening attachments. Never open an attachment unless it is expected even if it is from a trusted user.
- Exercise extreme caution when downloading files from the Internet. Only download from reputable sites.
- Exercise reasonable caution when installing files from removable media such as CDs. Even "shrink-wrapped" software has been known to contain viruses.
- Report all virus incidents to the IT Helpdesk. Provide the following information if known: virus name or type, extent of infection (single PC, LAN, etc.), source of virus, and potential recipients of infected material. *Note the distinction between receiving an e-mail message that contains a virus-laden attachment versus allowing a virus to infect a computer. Most active computer users receive e-mail messages that contain viruses on a daily or weekly basis. By knowing the proper way to dispose of these messages, users can prevent any harm from coming to the system. Only cases of infections need to be reported.*
- If a computer is known to be infected, remove it from the network until it can be disinfected.
- Perform regular backups of the data on individual desktop systems.
- If IT responds to a virus incident and finds that the infected desktop system is not running virus protection software, then the individual must agree to purchase, install and properly use the software to prevent future incidents.
- Keep personal use to a minimum to reduce the possibility of receiving a virus on a University-owned computer.
- Read the IT Appropriate Use Policy (www.olemiss.edu/ause.html). Allowing a computer system to become infected puts other University systems at risk and, in the extreme, is a violation of the IT Appropriate Use Policy.