Anti-Virus Protection for UM Computers

Summary/Purpose: The purpose of this policy is to describe the responsibilities of individuals, departments and the Office of Information Technology (IT) in ensuring the protection of 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, email (specifically, email 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 UM 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 (http://www.olemiss.edu/software).
- 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. There will be a charge of $50 per visit for more than two visits to the same desktop within a three-month period. 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, filter packets from infected systems so that they do not propagate through the campus network).
- Continue server-based solutions to stop the propagation of viruses through University systems and networks.

DEPARTMENTAL RESPONSIBILITIES

- Purchase virus protection software for desktops within the department, whether it be through the IT-negotiated solution (referred to in this policy as “participating departments”) or another option. The use of alternative options for virus protection must be approved by the Chief Information Officer or the Security Coordinator.
- Designate a local contact for departmental virus protection to assist in installation of virus protection software, education of the user community and virus response.
The University of Mississippi

- Schedule a mandatory-attendance workshop in which IT staff and the departmental contact train departmental users on protecting their systems.

INDIVIDUAL RESPONSIBILITIES

- Update virus protection software daily.
- Configure desktop system to perform frequent auto-scans for viruses (daily recommended).
- Exercise extreme caution when opening attachments. Never open an attachment unless it is expected even if it is from a trusted user.
- 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.
- Perform regular backups of the data on individual desktop system.
- 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.