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 type of malicious software, which is 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 external storage devices, CDs/DVDs, email (specifically, email attachments), and documents or applications downloaded from the Internet. Within the context of this document, the term "virus" is also inclusive of other related types of software, including malware, spyware, trojans, rootkits, and botnets.

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. Anti-virus software is an important tool to help safeguard your data. The guidelines provided in this policy are designed to help UM achieve a uniform security posture. This is in the interest of all parties, as it will help ensure effective incident response, efficient support, increased productivity, and robust protection of our information and systems.

IT RESPONSIBILITIES

- Provide a recommended solution for virus protection based on campus feedback, industry research, and the interest of UM as a whole.
    - Negotiate licenses that result in cost-effective solutions for campus units.
    - Provide an opportunity for participating 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.
    - Effectively communicate the recommended solution to departments. The current recommendation will be posted to the IT Security website (antivirus policy).
- Make available an option for individual purchase of the recommended solution through the FTDC (software for virus protection).
- Provide installation, training, and ongoing software support.
    - 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.
    - There will be a charge of $50 per visit for more than two visits to the same computer within a three-month period.
    - Requests for assistance from departments that choose not to participate in the IT recommended solution will be given a lower priority than requests from 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).
- Employ central server-based solutions that mitigate the risk of viruses and stop their propagation through UM systems and networks.

DEPARTMENTAL RESPONSIBILITIES

- Purchase and install virus protection software for UM owned computers.
    - While the IT recommended solution is always preferred, an alternate solution may be used instead, as long as the following caveats are upheld:
        - The alternate solution must be approved by the Chief Information Officer or Security Coordinator.
        - The alternate solution must meet the basic technical requirements below.
        - The department must ensure that the alternate solution continues to meet the basic technical requirements and is re-approved every two years.
- Designate a local contact for departmental virus protection. The contact will assist in installation of software, education of the user community, and incident response.

INDIVIDUAL RESPONSIBILITIES

- Update virus protection software daily, and configure computer systems 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, Server, LAN, etc.), source of virus, and potential recipients of infected material.
- Perform regular backups of data on individual computer systems (daily recommended).
- If IT responds to a virus incident and finds that the infected computer system is not running virus protection software, then the individual must agree to purchase, install and properly use the software to prevent future incidents.

TECHNICAL REQUIREMENTS

Most current virus protection solutions provide a holistic approach to endpoint-security. These commonly seen technical requirements are applicable to the IT recommended solution and any approved alternate solution.

- It should employ techniques including signatures, heuristics, and behavior detection.
- It should routinely scan local file systems, including all hard disks and attached storage. These scans should be scheduled on regular intervals.
- It should be capable of actively monitoring volatile memory (RAM).
- It should have the capability to prevent network-based attacks and exploitation. Ideally, this includes both firewall and intrusion detection modules.
- Both the anti-virus software and its signatures should be set to automatic update daily.
- The anti-virus component of the software should be configured to keep logs for a reasonable period of time. In the event of an incident, these logs may be needed to investigate potential data loss.

ADDITIONAL INFORMATION

See the Information Confidentiality/Security (Information Confidentiality/Security) and the IT Appropriate Use (IT Appropriate Use Policy) policies for additional information and related security requirements.