Malicious Software Prevention Policy

Purpose:

Information Security exists to further the mission of the University. The University is comprised of large and diverse populations with evolving needs related to information technology resources and data. University management is committed to safeguarding those resources while protecting and promoting academic freedom. Although intrinsic tension exists between the free exchange of ideas and information security, and can manifest itself in some circumstances, the following framework has been identified to promote the best balance possible between information security and academic freedom.

Malicious Software is a threat to the University's business operations and academic missions. The Malicious Software Policy establishes requirements necessary for maintaining the confidentiality, integrity and continuous availability of data and network resources at the University of Miami.

Scope:

This policy applies to all University employees, faculty, students, contractors, guests, consultants, temporary employees, and any other users, including all personnel affiliated with third parties, as well as any hardware devices used to access University data.

Definitions:

Malicious Software/Malware: Software sometimes known as malware is designed to penetrate and/or damage systems without the owner’s awareness and consent. Examples include: computer viruses, worms, Trojans, spyware, and rootkits.

System Administrator: An individual who performs network/system administration duties and/or technical support of network/systems that are accessed by other people, systems, or services. Only full-time and permanent part-time employees of the University and/or third party vendors approved by IT may function as system administrators.

Data Custodian: The person responsible for, or the person with administrative control over, granting access to an organization's documents or electronic files while protecting the data as defined by the organization's security policy or its standard IT practices.
University Member/Affiliate: Anyone associated with the University of Miami including employees, students, contractors, guests, consultants, temporary employees, and any other users, including all personnel affiliated with third parties University resources.

POLICY:

It is the policy of the University of Miami to implement controls on hardware used to fulfill academic needs and conduct University business, to prevent Malicious Software from disrupting the University’s operations. The controls are as follows:

- Anti-virus and anti-spyware/anti-adware software must be installed, active and maintained with up-to-date definitions on all University workstations, laptops and servers.
  Note: Anti-virus and anti-spyware software is available at no expense to the user for installation on personally owned devices that will be used to fulfill University academic and/or business needs.
- All files should be scanned in real time each time they are accessed including those located on removable storage devices, floppies, CDs, and network stores.
- Files that are excluded from real time and scheduled scans should be scanned in alternate ways. For example, an Exchange information store would not be scanned by a file-level scanner, but must be regularly scanned with an Exchange application level scanner.
- When malicious software or threat is found, the suspected files must be automatically removed from the system.
- All e-mail messages and attachments should be scanned for malicious software.
- Files downloaded from the Internet via the firewall should be scanned for malicious software.
- Server malicious software log files must be generated and maintained for a period of 1 year with 3 months of data online.
- If any users suspect that any malicious software is present on their workstation, laptop or a server, they should contact their local system administrator and/or Help Desk immediately for assistance.
- Users must report any other suspicious activity to their local system administrator and/or HelpDesk (e.g. erratic mouse movements, browser windows opening unexpectedly, etc.).

EXCEPTIONS:

Any requests for exceptions to this policy must be submitted in writing and will be reviewed on a case by case basis. Exceptions shall be permitted only after written approval from the responsible Vice President or Information Technology designee of the respective campus. The list of exceptions shall be reviewed annually and cancelled as required.

IMPLEMENTATION:

University Members/Affiliates:
- Responsible for adhering to requirements outlined in this policy.

System Administrator/Data Custodian:
• Responsible for ensuring systems and data are properly protected with appropriate software and updates.

Chief Information Security Office:
• Responsible for regular review of the Malicious Software Protection Policy. The review will occur annually or when significant changes occur.

Responsible Vice President or Information Technology designee:
• Responsible for reviewing and approving or denying exception requests.
• Responsible for reviewing exceptions yearly.
• Responsible for monitoring the enforcement of the policy.

SANCTIONS:

Accounts and network access may be administratively suspended with or without notice by the University when, in the University's judgment, continued use of the University's resources may interfere with the work of others, places the University or others at risk, or violates University policy.

Knowing violations of the policy will be addressed by disciplinary policies and procedures applicable to the individual.

All known and/or suspected violations must be reported to the applicable Systems Administrator, who will report, as appropriate, to the applicable department. All such allegations of misuse will be investigated by the appropriate University administrative office with the assistance of the Department of Information Technology and the Department of Human Resources.

Penalties may include:

• Suspension or termination of access to computer and/or network resources;
• Suspension or termination of employment, to the extent authorized by other university published policies and procedures;
• Suspension or termination of contract computer and/or network services; or
• Criminal and/or civil prosecution.

OTHER APPLICABLE POLICIES:

• Information Security Policy
• Information Technology Security Incident Response Notification Policy
• Information Technology Security Incident Response Procedures Policy