UNIVERSITY OF MIAMI

UNIVERSITY OF MIAMI POLICY AND PROCEDURE MANUAL

TITLE:	Malicious Software Protection Controls	REFERENCE:	Revised
CATEGORY:	Information Technology	PAGE:	1
		SUPERSEDES:	POL-UMIT-A170-013-01
APPROVER:	David Ertel Interim Senior Vice President Business and Finance	VERSION: EFFECTIVE:	2 May 16, 2017

I. **PURPOSE:**

Malicious Software is a threat to the University of Miami (University) business operations and academic missions and can result in the permanent loss of data, time to recover a system or the delay of important work. Protection from malicious code is necessary for maintaining the confidentiality, integrity and continuous availability of data and network resources at the University. The purpose of this policy is to establish requirements to protect University technology resources and data against intrusion by viruses and other malware.

II. **SCOPE:**

This document applies to University information technology (IT) assets and the employees, faculty, students, contractors, guests, consultants, temporary employees and any other users, including all personnel affiliated with third parties, who process, store, transmit or access these IT assets.

III. **POLICY:**

It is the policy of the University of Miami that computerized devices connected to the University network must use University approved malicious software protection controls and configurations. These computerized devices will be monitored for computer viruses and other malicious code. University of Miami Information Technology (UMIT) Services reserves the right to intercept and/or quarantine any network traffic or computing device that may pose a threat to University infrastructure, systems or data. This includes but is not limited to, files, messages, network traffic and devices.

Malicious Software Protection Controls:

1. Anti-virus/malware software must be installed, enabled, and configured for up-to-date definitions, scans and infection removal or quarantine on all Windows and Mac operating system computing devices that connect to the University network. All other non-Windows computing devices must use equivalent products.
2. A computing system unable to meet a requirement due to system limitations must be formally authorized by IT Security Operations. An exemption will require the server to sit behind a properly configured hardware firewall and meet compensating controls such as, enterprise class configuration, administration and maintenance requirements.

3. All University issued computing devices must use the malicious software protection controls installed and configured by UMIT Services. Users are prohibited from disabling or altering the effectiveness of the installed malicious software protection controls unless authorized by IT Security Operations.
4. Malicious software protection for personally owned devices used to fulfill University academic or business needs is available at no expense to University employees.
5. Automated system scans and definition updates will be performed on a periodic basis. In cases where this is not possible, the User or System Administrator is responsible for regularly initiating the scan and maintaining definition updates. Manual scans and definition updates require business justification and formal authorization by IT Security Operations.
6. All files should be scanned in real time when accessed, including files located on removable storage media, CDs, and network stores. Files that are excluded from real time scans should be scanned in alternate ways and on a periodic basis.
7. Inbound email messages and attachments will be scanned for malicious software. E-mail detected as a risk to the University community is blocked. Malicious software detection is not 100% and Users must exercise caution when opening email attachments.
8. Perimeter and application firewalls will be configured to perform malicious content scans.
9. An infected computing device must be immediately disconnected from the University wired and wireless network until the malware is removed in its entirety.
10. IT Security Operations must be notified of systems infected with Ransomware or other malicious software that is a threat to the University network and data.
11. The assessment and removal process for Ransomware or malicious software attacks that may compromise University data classified as confidential or protected by a legislative regulation may include hard drive removal for further analysis or reformat of the hard drive.
12. Data from a removed or reformatted hard drive may be restored from its latest data backup.

IV. DEFINITIONS:

Malicious Software: Software, sometimes known as malware, designed to penetrate systems without the owner’s awareness and consent with intent to destroy data, run destructive or intrusive programs or otherwise compromise the confidentiality, integrity, or availability of the victim’s data, applications or operating system. Examples include: computer viruses, worms, Trojans, ransomware, spyware, and rootkits.

Malware: A term derived from the works “malicious” and “software”. The expression is a general term used to refer to a variety of forms of hostile, intrusive, or annoying software or program code.

Privileged Account: A system user granted elevated privileged access with the ability to establish or modify application system policies, perform system administrative tasks and make global changes which can impact entire systems or processes.

Ransomware: a type of malware that prevents or limits users from accessing their computer system, either by locking the system’s screen or by locking the users’ files until a ransom is paid.

System Administrator: A person who manages the technical aspects of an information system and provides effective information system utilization, adequate security parameters and sound implementation. A system administrator includes any University Member with privileged account access that is above a normal user.

V. PROCEDURE:

1. It is the responsibility of the User to:
    a. Use reasonable precautions to prevent importing data onto computers that may contain malicious software.

    b. Ensure data stored on respective local computing device is backed up or copied to a University provided storage solution. If necessary, this data may be used to recover from a malicious software attack.

    c. Immediately report to the local system administrator and UMIT Service Desk any suspected downloads of malicious software present on their workstation, laptop or server or other suspicious activity, such as, mouse moves and clicks on its own, unwanted browser windows open unexpectedly, unusual messages or programs start automatically, system crashes, disabled anti-virus protection, etc.

2. It is the responsibility of the local system administrator to:
    a. Ensure data stored on respective servers is backed up at least on a daily basis and available for data recovery in the event of a malicious software attack.

    b. Ensure malicious software protection controls and firewall software is operating as required on respective servers and unnecessary services are disabled before operating in the production environment.

3. It is the responsibility of UMIT Services to
    a. Centrally manage University malware protection, detection and removal; hardware security scanning; and monitoring of firewall logs for computing devices and network equipment administered by UMIT.

    b. Maintain documentation of all authorized disabled or bypassed malicious software protection controls.

4. Chief Information Security Officer of designee (CISO) is responsible for monitoring the enforcement of the policy.

5. Violations

Violations of this policy and/or procedure will be addressed by the procedure applicable to the individual.

6. Other Applicable Policies:

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