UF UNIVERSITY of FLORIDA
Information Technology

POLICY

Policy: TS0007	Category: Technical Security	Version Date: 2/15/2017
Title: Malicious Software Controls		Effective Date: 2/22/2017
Originating Unit: Information Security Advisory Committee		Last Review: 2/15/2017
Review Resp: HIPAA Security Officer		Next Review: 2/22/2017

Purpose:

The purpose of this policy is to ensure that proactive security measures are taken to prevent and detect malicious software and that awareness is raised for recognizing and immediately reporting suspected occurrences of malicious software.

Scope:

This policy applies equally to all UF HSC information assets and to all UF HSC employees, contractors, and to all other users of Protected Health Information.

References:

1. UF Information Technology Security Policy, http://www.it.ufl.edu/policies
2. UF Information Security Incident Response Policy
3. UF Information Security Office Website: http://security.ufl.edu/

Policy:

1. The Unit Information Security Manager (ISM) is responsible to ensure that the Unit has written procedures to prevent and detect malicious software.
2. Any effects of malicious software shall be addressed in accordance with the UF Information Security Incident Response Policy.
3. All UF computing devices, whether connected to the network or stand-alone, must use malicious software protection controls and configurations approved by the Unit ISM. These include all workstations, servers and portable computing devices.
4. Malicious software protection controls:
   a. Must not be disabled or bypassed without formal authorization by the Unit ISM.
   b. Must not be altered in a manner that will reduce the effectiveness of the controls.
   c. Must not be altered to reduce the frequency of automatic updates.
   d. The Unit ISM shall maintain documentation of all authorized disabled or bypassed malicious software protection controls.
5. The Unit ISM shall ensure that:
   a. Recognized industry standards shall be used to combat malicious software.
   b. Malicious software protection controls are installed on every information system except in such cases where the Unit ISM determines that they should not be applied due to system limitations.

c. Updates and scanning engine updates are installed as soon as prudent, except in such cases where the Unit ISM determines that they should not be applied due to system limitations.
d. Only trained IT personnel will make changes or modifications to the configuration or function of the malicious software protection controls.
e. Malicious software protection training must be provided to all users in the Unit.
f. All software is scanned for malicious components using up-to-date protection controls before being loaded on any computing device.
g. A plan is developed and implemented to scan all computing devices on a periodic basis to ensure no unauthorized software is resident on any information system.
h. A plan is developed and implemented to verify that malicious software protection controls are tested periodically.
i. A plan is developed and implemented to scan all data imported onto computers through physical (floppy disks, tapes, memory cards) or electronic means (email, FTP, downloading from the web) for malicious software.

6. It shall be the responsibility of the User to:
   a. Use reasonable precautions to prevent importing data onto computers through physical (USB flash drives, memory cards, external disks, tapes) or electronic means (email, FTP, downloading from the web) that contain malicious software.
   b. Ensure that all portable computing devices or personal computers in their custody are running the malicious software protection controls specified by the Unit ISM.
   c. Immediately report to the ISM or UF Computer Security Incident Response Team any suspected or actual incidence of malicious software infection per the UF Information Security Incident Response Policy.