



NUMBER: 7.3.15

DATE: 04/01/2005

REVISION: 02/03/2010; 12/14/2011

PAGE: 1 of 2

SECTION: INFORMATION TECHNOLOGY

AREA: NETWORK SECURITY

SUBJECT: MALICIOUS SOFTWARE PREVENTIONS

PURPOSE

To protect the UAMS network from malicious software.

SCOPE

UAMS Workforce with Access to Confidential Information, including Electronic Protected Health Information (ePHI), for any purpose.

DEFINITIONS

Confidential Information includes information concerning UAMS research projects, confidential employee information, information concerning the UAMS research programs, proprietary information of UAMS, and sign-on and password codes for access to UAMS computer systems. Confidential information shall include Protected Health Information.

Electronic protected health information means individually identifiable health information that is:

- Transmitted by Electronic media
- Maintained in Electronic media

Malicious code means an executable application (e.g. Java applet or Active X control) designed to damage or disrupt an information system.

UAMS workforce means physicians, employees, volunteers, residents, students, trainees, visiting faculty, and other persons whose conduct, in the performance of work for UAMS, is under the direct control of UAMS, whether or not they are paid by UAMS.

To access any other terms or definitions referenced in this policy:

<http://hipaa.uams.edu/DEFINITIONS%20-%20HIPAA.pdf>

POLICY

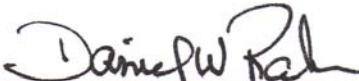
UAMS will maintain a documented process for appropriately guarding against, detecting, and reporting malicious software particularly viruses, worms and malicious codes that pose a risk to the UAMS network.

PROCEDURE

- A. The process for malicious software prevention, detection and reporting includes, but is not limited to:
1. Establishment of Active Directory policies and placement of intrusion detection and firewalls.
 2. Installation and updating of anti-virus software on all UAMS workstations, laptops, servers and other computing devices. Exceptions must be approved by IT Security.
 3. The examination of electronic mail attachments and data downloads for malicious software before use on UAMS information systems.
 4. An appropriate disaster recovery plan for recovering from malicious software attacks. Systems found to be infected with malicious software will be removed until the infection is removed.
 5. Procedures to limit unauthorized software installation. Use of peer to peer software file sharing applications is blocked on the UAMS firewall to reduce the risk of computer worms and illegal software.
 6. Home computers connecting to the UAMS network shall utilize local firewalls, and maintain updated anti-virus, anti-spyware, and operating system software. Instructions for the above can be found on the UAMS intranet at this link: http://intranet.uams.edu/it/How_To.asp.
- B. UAMS workforce members will be trained on and regularly reminded of the threat posed by malicious software, including, but not limited to:
1. How to identify malicious software
 2. How to report malicious software
 3. How to effectively use anti-virus software
 4. How to avoid downloading or receiving malicious software
 5. How to identify malicious software hoaxes
- C. UAMS workforce members must not by-pass or disable anti-virus software unless appropriately authorized.

SANCTIONS

Violation of this Policy will result in disciplinary action, in accordance with [Policy 4.4.02 Disciplinary Notice Policy](#).

Signature: 

Date: December 14, 2011