Oklahoma State University

Title: Protection from Malicious Software	**Policy #: SEC-04.02**
Category: HIPAA Compliance	**Authority: 45 CFR § HIPAA SECTION: 164.308(a)(5)(ii)(B)**
Standard: Security Awareness & Training	**Responsibility: Health Care Components**
Effective Date: 4/20/2005	**Page 1 of 2**
Approved By: OSU Legal Counsel	**Revised: 7/1/2013**

PURPOSE:

Ensure that workstations and servers operate within the security measures as adopted by the university.

POLICY:

Efficient use of computing resources is shared by every employee. The purpose of this policy is to outline the measures that will be taken to ensure that all network devices are operating with the configuration and standards necessary to maintain the integrity of the data and the privacy of privileged information. Each campus must have procedures in place for guarding against, detecting, and reporting malicious software. *§164.308(a)(5)(ii)(B)*

PROCEDURE:

Each PC used in a HIPAA regulated environment will have spyware/malware detection software installed. All patches/updates to the application and operating system will automatically be pushed to the devices from IT. Antivirus is installed and automatically updated.

Malware

1. OSU shall include in security training or via reminders information regarding malicious software, prevention of attack or inappropriate access by such software.
2. Staff shall be informed of appropriate use guidelines of OSU.
3. OSU staff shall be limited in use of software or access to internet sites or functions that increase the risk of malicious software
4. OSU will be monitoring PCs to determine that appropriate safeguards are in place to prevent such software, include standards for operating systems, firewall, antivirus software and operating system updates.
5. Records of updates and changes in these recommendations shall be maintained by the security officer as part of the IT inventory database.

Antivirus

Oklahoma State University

Title: Protection from Malicious Software	**Policy #: SEC-04.02**
Category: HIPAA Compliance	**Authority: 45 CFR § HIPAA SECTION: 164.308(a)(5)(ii)(B)**
Standard: Security Awareness & Training	**Responsibility: Health Care Components**
Effective Date: 4/20/2005	**Page 2 of 2**
Approved By: OSU Legal Counsel	**Revised: 7/1/2013**

OSU is committed to taking the necessary steps to prevent computer viruses. Employees must adhere to the policies and procedures listed below:

- Employees must scan files attached to email messages, files downloaded from the Internet, and files on diskettes using the antivirus program supplied by OSU.
- The System Administrator or Security Official must conduct a virus scan of the OSU computer network servers and workstations at least once a week. Employees should be instructed to log off, but not shut down their workstations once a week so the anti-virus software program can run in the evening.
- When OSU purchases new computer software, the System Administrator or Security Official will test the application for viruses.
- The System Administrator or Security Official must make sure that diskettes used to store computer software programs are "write-protected" or protected against information from being saved on this disk. This prevents viruses from being copied onto diskettes containing important information.
- If OSU obtains a recycled computer that comes pre-loaded with software or if the hard drive is pre-formatted, the System Administrator, Security Official, or information technology consultant will scan the hard drive for viruses and other vulnerabilities.
- All software should be acquired from reputable dealers.