Scope

Indiana University Health Sciences (IUHS)

All employees and faculty of IUHS, as well as vendors, contractors, partners, students, collaborators, and any others doing business or research with IUHS, will be subject to the provisions of this policy. Any other parties, who use, work on, or provide services involving IUHS computers and technology systems will also be subject to the provisions of this policy. Every user of IUHS computer resources is expected to know and follow this policy.

Policy Statement

1. All IUHS computer devices connected to the Indiana University network (herein referred to as "the network") or networked resources shall have anti-virus software installed, configured so that the virus definition files are current, routinely and automatically updated; and the anti-virus software must be actively running on these devices.
2. All files on computer devices will be scanned periodically for viruses. Schools, centers, departments, and practice plans will establish a schedule for automatically scanning the devices within their control.

3. If deemed necessary to prevent propagation to other networked devices or detrimental effects to the network or data, an infected computer device may be disconnected from the network until the infection has been removed. This will be done under the direction of the Chief Information Security Officer in conjunction with the affected school, center department or practice plan and the University Information Security Office.

4. Exceptions to this policy may be allowed if a school, center, department, or practice plan computer device cannot have anti-virus software installed. Possible examples of this would be vendor-controlled systems, FDA validated systems, or devices where anti-virus software has not yet been developed. In these cases, the unit must develop a plan to protect the device from infection.

5. An exception may be granted if an infected computer device is discovered that performs a critical function and may not be immediately taken "offline" without seriously impairing some business function or affecting patient care. Under those circumstances, a plan will be developed to allow the computer device to be taken offline and the infection purged while protecting the function of the device.

---

**Reason for Policy**

This policy is designed to help prevent infection of IUHS computers and computer systems by computer viruses and other malicious code. This policy is intended to help prevent damage to user applications, data, files, and hardware.

---

**Definitions**

*Computer devices* are any type of device connected to a network that could become infected with a computer virus. Examples of computer devices would be, but not limited to: workstations, servers, laptops, etc.

*Malicious software* is any type of computer code that infects a machine and performs a malicious action. This is sometimes perpetrated by computer viruses, worms, Trojans, etc.

*Anti-Virus software* runs on either a server or workstation and monitors network connections looking for malicious software. Anti-virus software is generally reactive, meaning a signature file must be developed for each new virus discovered and these virus definition files must be sent to the software in order for the software to find the malicious code.
Virus definition files are periodic files provided by vendors to update the anti-virus software to recognize and deal with newly discovered malicious software.

Sanctions

If it is suspected that this policy is not being followed, report the incident to a departmental manager or representative and the Chief Information Security Officer.

Any exceptions to this policy must be approved in advance by both the Chief Information Security Officer and the Associate Vice President for Information Technology, Clinical Affairs IT Services.

Any person found to have violated this policy will be subject to appropriate disciplinary action as defined by the provisions of Indiana University Policy IT-02, Misuse and Abuse of Information Technology Resources.

History

1. IUSM SEC-09, April 25, 2005, initial policy.
2. Policy reviewed on February 24, 2011.
5. Policy scope edited, expanded to include Health Sciences, August 5, 2014.