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.

IUHS computing resources have been developed to encourage widespread access and distribution of data and information for the purpose of accomplishing the educational, clinical, and research missions of the school. This policy will not supersede any Indiana University developed policies but may introduce more stringent requirements than the university policy.

Policy Statement
1. All networked devices belonging to or managed by IUHS schools, departments, centers, practice plans, or other affiliated and partner organizations will be patched with vendor-provided operating system security patches.

2. These patches will be applied as soon as possible following appropriate testing of the security patches by the IUHS schools, departments, centers, practice plans, or other affiliated and partner organizations.

3. New devices must be tested and patched to the current patch level, as defined by the operating system vendor, prior to the device being connected to the production network.

4. Current patch status for all IUHS schools, departments, centers, practice plans, or other affiliated and partner organizations must be managed by the appropriate unit within CAITS. Devices that cannot be patched will have the exact mitigation effort documented by the appropriate unit within CAITS.

---

**Reason for Policy**

This policy is designed to ensure that computer systems attached to the Indiana University network are updated accurately and timely with security protection mechanisms (patches) for known vulnerabilities and exploits. These mechanisms are intended to reduce or eliminate the vulnerabilities and exploits with limited impact to the business.

---

**Definitions**

*Operating System (OS)* is the set of programs used to provide the basic functions of a computer.

*A device* is defined as any object used to store, process, and/or transfer data.

*Confidentiality, Integrity, Availability (CIA)* are the three basic tenets of information security.

*A networked device* is defined as any device that is either permanently or periodically attached to the Indiana University network.

*Remediated* is defined as all patches required by the vendor that have been applied.

*Mitigated* is defined as steps have been taken to protect a device from a particular vulnerability, i.e., the device has been removed or otherwise isolated from the network, the NIC card has been removed, or an approved deviation from the required patch process has been approved by the Chief Information Security Officer.
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-10, 24 Oct 2005, first draft of policy.
2. Policy reviewed on February 24, 2011.
5. Policy scope edited, expanded to include Health Sciences, August 5, 2014.