MEHARRY MEDICAL COLLEGE

**POLICIES**

**Effective Date: January 31, 2008**

**Retired:**

**Revised: October 1, 2013**

**Approved by: A. Cherrie Epps, Ph.D.**
**President and Chief Executive Officer**

**Subject: Office of Information and Technology - Security Patch Policy**

**SCOPE:**
The Vice President of Information Technology (VP) is designated as the institutional officer responsible for specifying standards for access and acceptable use of information technology resources.

**POLICY STATEMENT:**
This standard identifies the need to apply vendor-issued critical security updates and patches regularly to protect College data and systems. It applies to all electronic devices connected to the College network including computers, network switches and routers, personal digital assistant devices, laptop computers, etc.

**Applicability:** This policy is applicable to all Meharry Medical College students, faculty and staff and to bona fide associates granted use of Meharry Medical College telephone resources.

**PURPOSE:**
Almost all operating systems and many software programs have periodic security patches released by the vendor that need to be applied. If critical patches and updates are not applied on a regular basis, computers on the College network risk being vulnerable to various worms, viruses, Trojans, and direct hacker attacks. The result can be loss of data, denial of service for other users, or attacks directed at other Internet users from the compromised machine.

**DEFINITIONS:**
**Authorized Use**: authorized use of Meharry Medical College owned, leased, operated, or contracted computing and network resources is used consistent with the education, research, and administrative mission of the College and is consistent with this policy.

**Authorized Users:** authorized users are current students, faculty and staff of the College.

**Patch:** A software update, usually provided by the software publisher, which is intended to correct functional or security issues in a software program.

**CO:** Compliance Officer, the enforcing unit for the Computer and Network Usage Policies

at Meharry Medical College.

**MMC:** Meharry Medical College (alias the College) for which the policy manual applies.

**IT:** Information Technology, the source for establishing the Computer and Network Policies at Meharry Medical College.

**POLICY:**
Software patches must be installed in a timely manner in order to ensure the continued functionality and security of programs installed on Meharry computer or network resources.

**PROCEDURE:**
Computers and other electronic devices attached to the College network must be regularly maintained including the application of critical security patches within 60 days after release by the vendor. Computers and other electronic devices with non-public or sensitive data must have critical patches applied more frequently. Other patches not designated as critical by the vendor must be applied on a normal maintenance schedule, which may depart from the above.

Many vendors have automated the patching procedure, particularly for desktop computers. While there is some potential for error by the vendor, the risks are substantially greater than if patches are never applied at all due to oversight. IT staff will also deploy patches remotely. In some circumstances, the Meharry Help Desk may install patches on users' computers.

Patches on production systems (e.g. servers) may require complex testing and installation procedures. In certain cases, risk mitigation other than patches is preferable. The risk mitigation alternative selected should be in proportion to the risk. The reason for any departure from the above standard and alternative protection measures taken must be documented in writing for devices storing non-public data.

On "Patch Tuesday" (second Tuesday of the month), the Systems Administrator (SA) monitors the new patches issued by Microsoft. Although Workstation patches are released for immediate installation using a local Windows Server Update Services (WSUS) server, Server patches are held back one to two weeks to monitor any adverse effects industry wide. Server patches are then applied on the third or fourth Friday of each month. The Server's "Automatic Updates" policy is set to automatically download patches from the WSUS server, but the SA has to manually apply the patch. A reboot is also manually initiated after midnight by the SA. Once the servers are back up, the SA logs

onto the server to verify that all the services have been properly re-started. Applying patches on Fridays gives the SA the weekend to troubleshoot any issues that may arise.

The regular application of critical security patches is reviewed as part of the normal College audit procedures. The Meharry Help Desk can be contacted for additional questions by dialing HELP (4357).

**SANCTIONS:**
Violations of this policy are subject to disciplinary action up to or including termination in accordance with Meharry Medical College personnel policies and procedures.

**EXHIBITS:**