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 – Clinical Computing Policy

SCOPE:
The Vice President for Information Technology (VP) is designated as the institutional officer responsible for identifying standards for access and acceptable use of information technology resources. This standard defines the use of backup software and procedures necessary for the protection of the College's computer systems and data. Inadequate backup policies and procedures represent a substantial risk to the Meharry community in terms of time, money, and potential data loss. To protect against the loss of data on College servers and reduce institutional risk, the VP has approved a set of backup policies and procedures specific to each type of server.

POLICY STATEMENT:
Administrators of Meharry Medical College server resources have a responsibility to protect information residing on those resources from intentional or accidental deletion. This policy provides guidelines for the appropriate application and use of backup solutions**.**

Applicability: This policy is applicable to all Meharry Information Technology administrators and staff who are involved in the administration or operation of the College's servers.

PURPOSE:
Data can be destroyed by system malfunction, accidental or intentional means. Adequate backups will allow data to be readily recovered as necessary. In order to minimize any potential loss or corruption of this data, units responsible for providing and operating administrative applications need to ensure that data is adequately backed up by establishing and following appropriate system backup procedures.

This Backup Policy establishes the guidelines and procedures to be followed to ensure proper backup and storage of electronic information.

DEFINITIONS:
Back-up: The saving of files onto magnetic tape or other off line mass storage media for the purpose of preventing loss of data in the event of equipment failure or destruction.

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 (1) current students, faculty and staff of the College; (2) anyone connecting to a "public" Information Technology Station (ITS) or kiosk, and (3) others who have been authorized to use a particular resource by the campus unit responsible for operating that resource.

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.

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

Virus: A virus is any computer file or section of programming code which causes loss or corruption of data on a computer without the user intending for it to be done. Viruses are spread in e-mail attachments, as downloads, and in various other ways. It is common for a user of a computer not to realize until it is too late that a virus has infected the computer. Once the damage has been done, it is often difficult or impossible to retrieve all of the data originally on that computer.

POLICY:

General Principles
Users and administrators of computing resources at Meharry Medical College are responsible for ensuring that those resources are not adversely affected by accidental or intentional loss or alteration.

Systems Covered:
This policy covers hardware and software maintained by the Office of Information Technology. This includes laptops, hand-held computing equipment, desktop computers, server and core database storage systems and networks necessary for the operations of the campus. Backup procedures should be documented for the following systems:

- Banner HP-UX Databases

- HP-UX operating Software
- Banner Server Applications
- Web-Focus Server Applications
- Work-Flow Server Applications
- McKesson Databases
- McKesson HP-UX operating Software
- All Meharry Servers
- Network Servers

PROCEDURE:

Backup cycles will be determined in conjunction with the business owner of each data system. This evaluation will include an assessment of the data sensitivity and criticality for the College. All tapes will be labeled and dated according to their system name.

Full back-ups are performed nightly on Monday, Tuesday, Wednesday, Thursday and Friday. If for maintenance reasons, backups are not performed on Friday, they shall be done on Monday. Off line tapes used for nightly back-up shall be stored in a fireproof safe. Monthly backup tapes shall be stored off campus.

Except when otherwise indicated, Backup Procedures should address the following:

Frequency

- Daily incremental backup - to be retained for a period of 4 weeks.
- Full Weekly Backup - to be retained for a period of 6 weeks.
- Full monthly backup 1st week - to be retained for a period of 16 weeks.
- Monthly backup for July - to be retained for a period of 10 years.
- Monthly backup Jan, Apr, Oct - to be retained for a period of 1 year.

Backup Software used

- Current vendor contact information
- When new releases are due to be shipped
- If and when current licenses for backup software expire

Backup Logs / Media Labeled

- Record details of files backed up, files skipped, and tapes used

Media Handling Policies

- Rotate backup tapes
- Physically damaged or corrupt tapes are to be destroyed in an approved

secure manner
- Two complete sets of backup tapes to be rotated off site as per the appropriate policy

Archives
Archives are made at the end of every year in June. User account data associated with the file and mail servers are archived one month after they have left Meharry Medical College.

Restoration
Users that need files must submit a request to the Help Desk include info about the file creation date, the name of the file, the last time it was changed, and the date and time it was deleted or destroyed.

Verification
The Director for Computer Operations shall delegate a member of the IT Department to perform regular back-ups. The delegated person shall:

- Verify on a weekly basis that the backup schedule is operating as per the minimum requirements listed above. Verify that it is possible to restore files from backup tapes twice per year, for each system and ensure that the correct file protection and file ownership controls are present in the restored files. Verify that backup data from older backups can be retrieved by scanning backup tapes.

EXHIBITS: None.