HACKETTSTOWN REGIONAL MEDICAL CENTER
Administrative Policy & Procedure
Systems Data File Use Procedure

==

Effective Date:	**March 2000**	**Policy No:**	**IS06**
Cross Referenced:		**Origin:**	**Information Systems**
Reviewed Date:	**11/03, 05/05, 01/08, 10/12**	**Authority:**	**Chief Operating Officer**
Revised Date:		**Page:**	1 of 2

PURPOSE:

Provide a secure environment regarding data files created for Hackettstown Regional Medical Center (HRMC) business use.

POLICY:

The scheduling and implementation of routine file backups for data files on all local (non-networked) microprocessors, is the responsibility of the Department Manager. Criticality of these files should be determined and a schedule implemented accordingly. All files located on network servers will be backed up daily by IS and archived in a secure environment

PROCEDURE:

1.   The end user is responsible for determining and maintaining data file structures for all non-networked systems based on the required results.

2.   It is the responsibility of the individual department or user to identify critical files and implement necessary backup procedures to secure the data if the files are maintained in local mode. Optimal procedures would include files to reside on a network drive providing automatic daily backup.

3.   Information Systems is responsible for file backup of all HRMC network secured system files located on network servers.

- Servers are backed up using Datavault Backup Software. The data is backed up to one of 2 Vaults located in the HRMC Datacenter.

   Vault Information:

Vault Name	IP Address
VABE-1	10.12.32.50
VABE-2	10.12.32.73

- These Vaults are then replicated to partners located at the Venyu datacenter in Baton Rouge, LA. or the Anthelio SEDC Datacenter in Springfield, MO.
- Normal Server backups are performed on a daily basis and have a 1 year retention time consisting of Daily, Weekly, and Monthly Backups.
- Database Backups are configured by the Anthelio Database Group and usually consist of a Dump to Disk, which is then backed up by Datavault during the regular Daily Backup. Special backup jobs for Transaction logs etc. are set up as needed and usually have a 48 hour retention time.
- Backups are monitored by Nimbus and e-mails are sent from the Datavault System in the event that a Backup fails.
- Backups are configured using the Datavault Agent Console that is installed on the VABE-1 Vault. This is also where Restores are started and Logs can be found.

==

Effective Date:	**March 2000**	**Policy No:**	**IS06**
Cross Referenced:		**Origin:**	**Information Systems**
Reviewed Date:	**11/03, 05/05, 01/08, 10/12**	**Authority:**	**Chief Operating Officer**
Revised Date:		**Page:**	2 of 2

4. All network file structures are the responsibility of the IS Department. Network file maintenance, including purging and archiving, is monitored and maintained by the IS Department. Access to these network functions are controlled by IS.

5. User access to systems, data and computer files will require following the procedures for Computer Systems Access.